TANDBERG

Video Communication Server



ADMINISTRATOR GUIDE

Version X3.0
July 2008

What's in this Manual?

What's in this Manual?

What's in this Manual?

What's in this Manual?

What's in this Manual?

What's in this Manual?

Firewall Traversal

Legal Notices

Disclaimer

The specifications for the product and the information in this Administrator Guide are subject to change at any time, without notice, by TANDBERG.

Every effort has been made to supply complete and accurate information in this Administrator Guide, however, TANDBERG assumes no responsibility or liability for any errors or inaccuracies that may appear in this document.

Intellectual Property Rights

This Administrator Guide and the product to which it relates contain information that is proprietary to TANDBERG and its licensors. Information regarding the product is found adjacent in the Copyright Notice and Patent Information sections.

This Administrator Guide may be reproduced in its entirety, including all copyright and intellectual property notices, in limited quantities in connection with the use of the product. Except for the limited exception set forth in the previous sentence, no part of this Administrator Guide may be reproduced, stored in a retrieval system, or transmitted, in any form, or by any means, electronically, mechanically, by photocopying, or otherwise, without the prior written permission of TANDBERG. Requests for such permission should be addressed to ipr@tandberg.com.

TANDBERG® is a registered trademark belonging to Tandberg ASA. Other trademarks used in this document are the property of their respective holders.

Philip Pedersens vei 22
1366 Lysaker
Norway

Tel: +47 67 125 125

Fax: +47 67 125 234

e-mail: tandberg@tandberg.com

Copyright Notice

The product that is covered by this Administrator Guide is protected under copyright, patent, and other intellectual property rights of various jurisdictions.

This product is

This product includes copyrighted software licensed from others. A list of the copyright notices and the terms and conditions of use can be found at:

http://www.tandberg.com/collateral/documentation/User_Manuals/TANDBERG VCS EULA.pdf

and

http://www.tandberg.com/collateral/documentation/User_Manuals/TANDBERG VCS Copyrights.pdf.

IMPORTANT: USE OF THIS PRODUCT IS SUBJECT IN ALL CASES TO THE COPYRIGHT RIGHTS AND THE TERMS AND CONDITIONS OF USE REFERRED TO ABOVE. USE OF THIS PRODUCT CONSTITUTES AGREEMENT TO SUCH TERMS AND CONDITIONS.

Patent Information

This product is covered by one or more of the following patents:

- EP01953201
- GB1338127

Other patents pending.
Contact tandberg@tandberg.com for an up-to-date list.

Safety Instructions and Approvals

Safety Instructions

For your protection please read these safety instructions completely before you connect the equipment to the power source. Carefully observe all warnings, precautions and instructions both on the apparatus and in these operating instructions. Retain this manual for future reference.

Water and Moisture

- Do not operate the apparatus under or near water – for example near a bathtub, kitchen sink, or laundry tub, in a wet basement, near a swimming pool or in other areas with high humidity.
- Never install jacks for communication cables in wet locations unless the jack is specifically designed for wet locations.
- Do not touch the product with wet hands.

Cleaning

- Unplug the apparatus from communication lines, mains power-outlet or any power source before cleaning or polishing.
- Do not use liquid cleaners or aerosol cleaners. Use a lint-free cloth lightly moistened with water for cleaning the exterior of the apparatus.

Ventilation

- Do not block any of the ventilation openings of the apparatus. Never cover the slots and openings with a cloth or other material. Never install the apparatus near heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat.
- Do not place the product in direct sunlight or close to a surface directly heated by the sun.

Lightning

Never use this apparatus, or connect or disconnect communication cables or power cables during lightning storms.

Dust

Do not operate the apparatus in areas with high concentration of dust.

Vibration

Do not operate the apparatus in areas with vibration or place it on an unstable surface.

Power Connection and Hazardous Voltage

- The product may have hazardous voltage inside. Never attempt to open this product, or any peripherals connected to the product, where this action requires a tool.
- This product should always be powered from an earthed power outlet.
- Never connect attached power supply cord to other products.
- In case any parts of the product has visual damage never attempt to connect mains power, or any other power source, before consulting service personnel
- The plug connecting the power cord to the product/power supply serves as the main disconnect device for this equipment. The power cord must always be easily accessible.
- Route the power cord so as to avoid it being walked on or pinched by items placed upon or against it. Pay particular attention to the plugs, receptacles and the point where the cord exits from the apparatus.
- Do not tug the power cord.
- If the provided plug does not fit into your outlet, consult an electrician.
- Never install cables, or any peripherals, without first unplugging the device from it's power source.

Servicing

- Do not attempt to service the apparatus yourself as opening or removing covers may expose you to dangerous voltages or other hazards, and will void the warranty. Refer all servicing to qualified service personnel.
- Unplug the apparatus from its power source and refer servicing to qualified personnel under the following conditions:
  - If the power cord or plug is damaged or frayed.
  - If liquid has been spilled into the apparatus.
  - If objects have fallen into the apparatus.
  - If the apparatus has been exposed to rain or moisture
  - If the apparatus has been subjected to excessive shock by being dropped.
  - If the cabinet has been damaged.
  - If the apparatus seems to be overheated.
  - If the apparatus emits smoke or abnormal odor.
  - If the apparatus fails to operate in accordance with the operating instructions.

Accessories

Use only accessories specified by the manufacturer, or sold with the apparatus.

Approvals

Electromagnetic Compatibility (EMC)

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

EC Declaration of Conformity

Manufacturer:	TANDBERG Telecom AS
Product Name:	TANDBERG Video Communication Server
Type Number:	TTC2-04
Description:	Network unit

This product complies with Commission Directives:

- LVD 73/23/EEC
- EMC 89/336/EEC

This product complies with harmonized Standards:

- EN 60950-1 : 2001, A11
- EN 55022 : 1998, A1/A2
- EN 55024 : 1998, A1/A2
- EN 61000-3-2 : 2000
- EN 61000-3-3 : 1995, A1

Technical Construction File No.: X14182

Year which the CE mark was affixed: 2007

For an official, signed version of this document, or details regarding documentation from the technical construction file, please contact TANDBERG.

JATE Approval (Japan only)

This unit must be connected to the public internet via a router/switch that has JATE approval.

Environmental Issues

Thank you for buying a product which contributes to a reduction in pollution, and thereby helps save the environment. Our products reduce the need for travel and transport and thereby reduce pollution. Our products have either none or few consumable parts (chemicals, toner, gas, paper). Our products are low energy consuming products.

TANDBERG's Environmental Policy

Environmental stewardship is important to TANDBERG's culture. As a global company with strong corporate values, TANDBERG is committed to following international environmental legislation and designing technologies that help companies, individuals and communities creatively address environmental challenges.

TANDBERG's environmental objectives are to:

- Develop products that reduce energy consumption, CO_2 emissions, and traffic congestion
- Provide products and services that improve quality of life for our customers
- Produce products that can be recycled or disposed of safely at the end of product life
- Comply with all relevant environmental legislation.

European Environmental Directives

As a manufacturer of electrical and electronic equipment TANDBERG is responsible for compliance with the requirements in the European Directives 2002/96/EC (WEEE) and 2002/95/EC (RoHS).

The primary aim of the WEEE Directive and RoHS Directive is to reduce the impact of disposal of electrical and electronic equipment at end-of-life. The WEEE Directive aims to reduce the amount of WEEE sent for disposal to landfill or incineration by requiring producers to arrange for collection and recycling. The RoHS Directive bans the use of certain heavy metals and brominated flame retardants to reduce the environmental impact of WEEE which is landfilled or incinerated.

TANDBERG has implemented necessary process changes to comply with the European RoHS Directive (2002/95/EC) and the European WEEE Directive (2002/96/EC).

Waste Handling

In order to avoid the dissemination of hazardous substances in our environment and to diminish the pressure on natural resources, we encourage you to use the appropriate take-back systems in your area. Those systems will reuse or recycle most of the materials of your end of life equipment in a sound way.



TANDBERG products put on the market after August 2005 are marked with a crossed-out wheelie bin symbol that invites you to use those take-back systems.

Please contact your local supplier, the regional waste administration, or http://www.tandberg.com/recycling if you need more information on the collection and recycling system in your area.

TANDBERG's Recycling Policy

As part of compliance with the European WEEE Directive, TANDBERG provides recycling information on request for all types of new equipment put on the market in Europe after August 13th 2005.

Please contact TANDBERG and provide the following details for the product for which you would like to receive recycling information:

- Model number of TANDBERG product
- Your company's name
- Contact name
- Address
- Telephone number
- E-mail

Digital User Guides

TANDBERG is pleased to announce that we have replaced the printed versions of our User Guides with a digital CD version. Instead of a range of different user manuals, there is now one CD – which can be used with all TANDBERG products – in a variety of languages. The environmental benefits of this are significant. The CDs are recyclable and the savings on paper are huge. A simple web-based search feature helps you directly access the information you need. In addition, the TANDBERG video systems now have an intuitive on-page help function, which provides a range of useful features and tips. The contents of the CD can still be printed locally, whenever needed.

产品中有毒有害物质表

部件名称	有毒有害物质或元素					
	铅	汞	镉	六价铬	多溴联苯	多溴二苯醚
金属部件	X	O	O	O	O	O
印刷电路板及组件	X	O	O	O	O	O
线缆和线缆组装	X	O	O	O	O	O
显示器（包括照明灯）	X	X	O	O	O	O

说明:

O：表示该有毒有害物质在此部件所有均质材料中的含量均在中国标准《电子信息产品中有毒有害物质的限量要求》(SJ/T 11363-2006) 所规定的限量要求以下。

X：表示该有毒有害物质至少在该部件的某一均质材料中的含量超出中国标准《电子信息产品中有毒有害物质的限量要求》(SJ/T 11363-2006) 所规定的限量要求。

注意：在所售产品中未必包含所有上述所列部件。

除非在产品上有另外特别的标注，以下标志为针对所涉及产品的环保使用期限标志。环保使用期限只适用于产品在产品手册中所规定的使用条件。

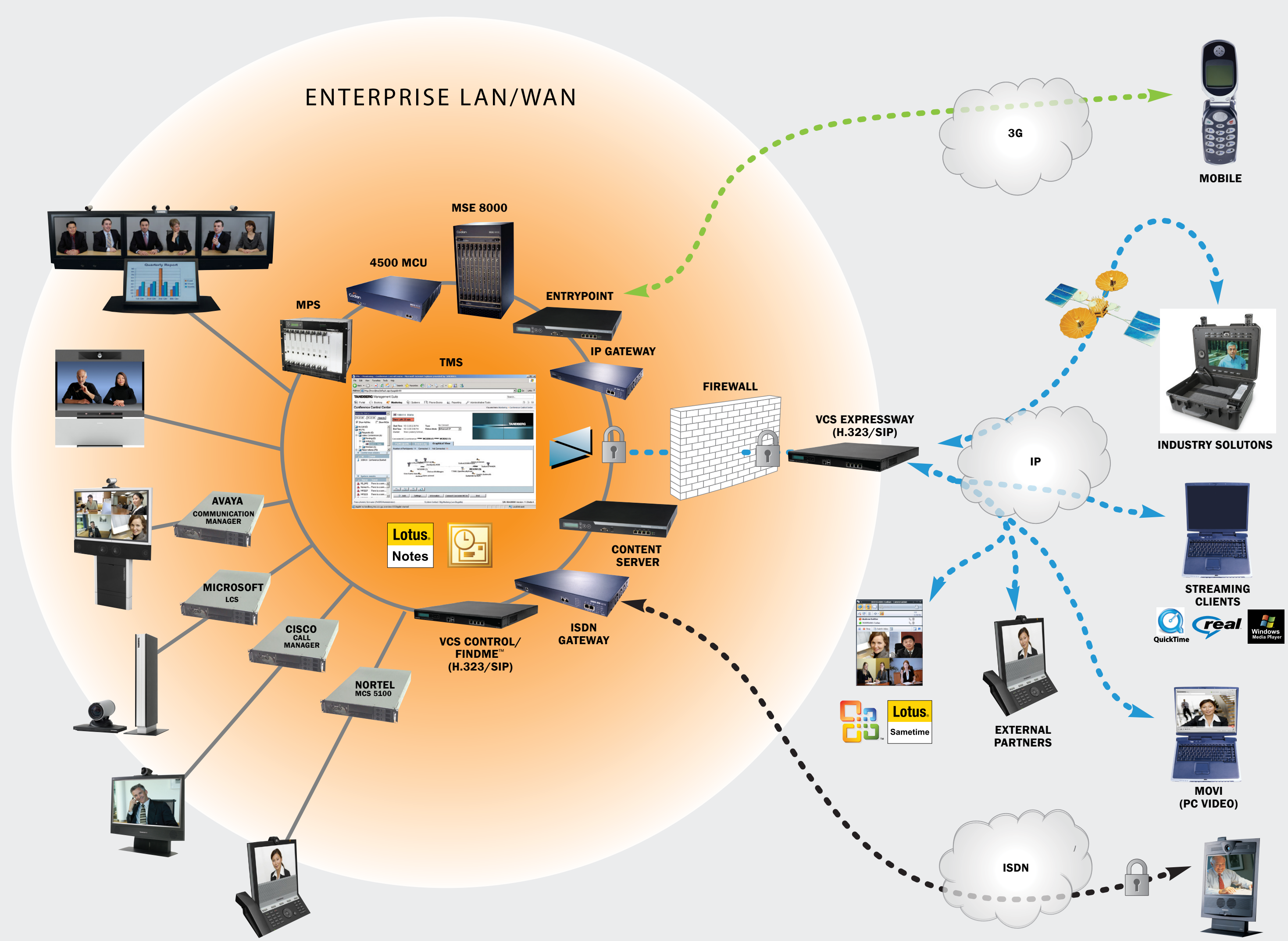
20

The TANDBERG VCS

Overview

The TANDBERG Video Communication Server (VCS) enhances the video experience and provides seamless communication between SIP and H.323 devices utilizing IETF and ITU standards. The VCS is the center of the video communication network, and connects all H.323 and SIP endpoints, infrastructure, and management devices. The VCS provides unrivaled scalability and redundancy to video communications, and is integral to TANDBERG interoperability with unified communications and Voice over IP systems. The VCS can be deployed with either the Control application or the Expressway™ application, with various optional packages including FindMe™ and Dual Network Interfaces.

VCS and the TANDBERG Total Solution

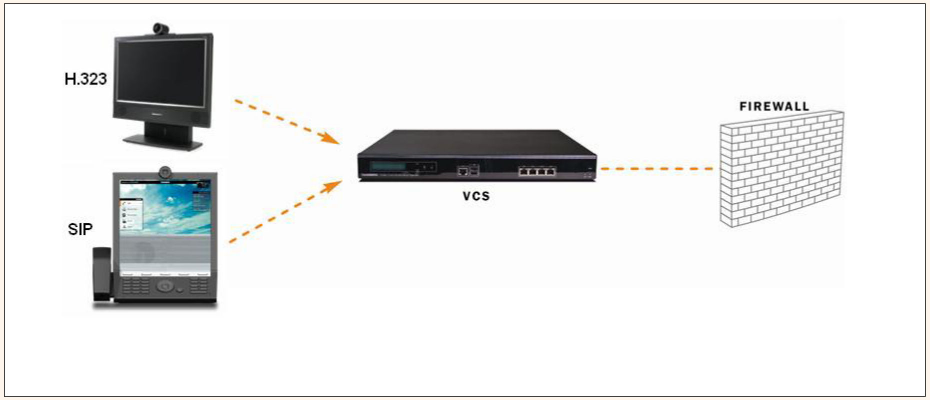


VCS Base Applications

VCS Control

The VCS Control provides internal video control and administration for all SIP and H.323 devices. It is normally deployed within your wide area network with endpoints that are behind the same firewalls or NAT devices.

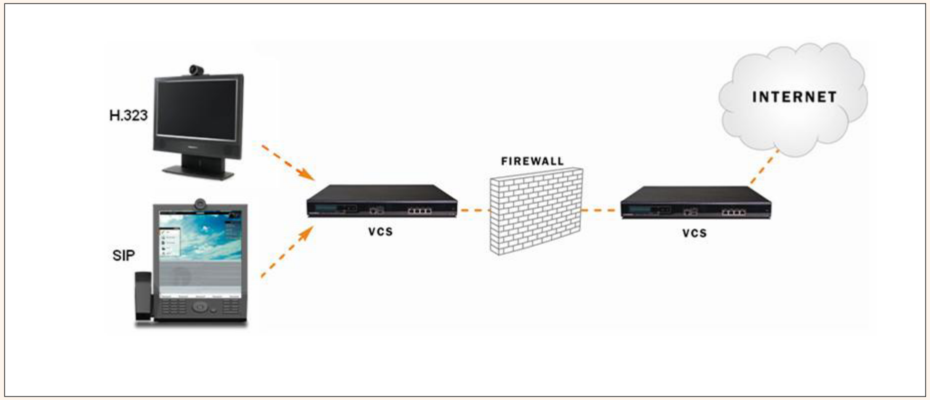
The VCS Control replaces the need to have separate H.323 gatekeeper, SIP registrar and H.323 - SIP gateway servers.



VCS Expressway™

The VCS Expressway provides standards-based firewall traversal for SIP and H.323 devices allowing secure firewall traversal of any firewall or NAT device. As well as all the functionality of a VCS Control, it also provides registration of traversal-enabled devices and STUN Discovery and STUN Relay services.

The VCS Expressway is normally deployed outside of your firewall or within the DMZ.



Standard Features

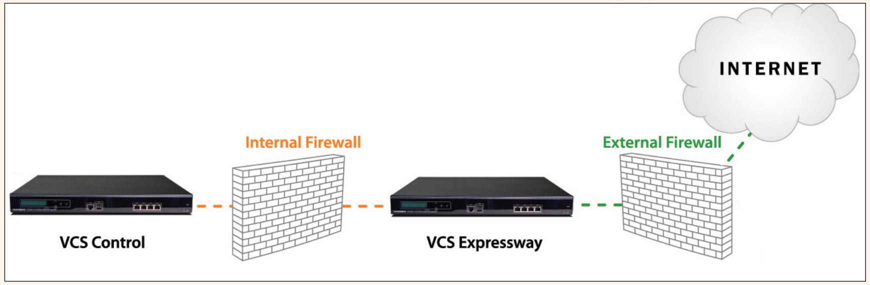
- H.323 gatekeeper
- SIP Proxy/Registrar
- SIP Presence Server
- SIP Presence User Agent
- SIP and H.323 support, including SIP/H.323 gatewaying
- IPv4 and IPv6 support, including IPv4/IPv6 gatewaying
- Bandwidth management on both a per-call and a total usage basis, configurable separately for calls within the local subzones and to external systems and zones
- Automatic downspeeding option for calls that exceed the available bandwidth
- URI and ENUM dialing via DNS, enabling global connectivity
- Up to 2500 registrations
- Up to 500 non-traversal calls
- Up to 100 traversal calls
- Up to 200 external zones
- Flexible zone configuration with prefix, suffix and regex support
- Can function as a stand-alone VCS or be neighbored with other systems such as VCSs, Border Controllers, gatekeepers and SIP proxies
- Can be part of a Cluster of up to 6 VCSs for increased capacity and redundancy
- Intelligent Route Director for single number dialling and network failover facilities
- Optional endpoint authentication
- Control over which endpoints are allowed to register
- Administrator Policy including support for CPL
- Embedded setup wizard via a serial port for initial configuration
- System administration via a web interface or RS-232, Telnet, SSH, and HTTPS
- Can be managed with TANDBERG Management Suite 12 or newer.

Optional Features

Dual Network Interfaces

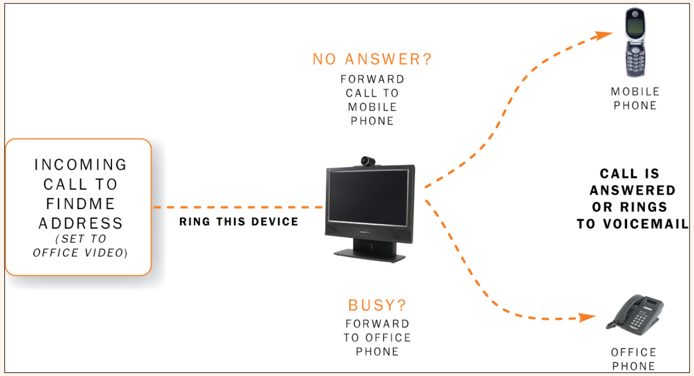
Enables the LAN 2 ethernet port on the VCS Expressway, allowing you to have a secondary IP address for your VCS.

This configuration is intended for high-security deployments where the VCS Expressway is located in a DMZ between two separate firewalls on separate network segments.



User Policy (FindMe™)

A unique industry solution that gives individual video users a single alias on which they can be contacted regardless of location. Users have the ability to log on to a Web-based interface and control where and how they are contacted.



What's New in this Version?

The following features have been introduced in version X3.0 of the VCS software:

Presence

Two new presence services are now supported: Presence Server and Presence User Agent.

Presence Server

- complies with IETF's SIP-based SIMPLE protocol
- supports PUBLISH, SUBSCRIBE and NOTIFY messages
- includes a Presence Server database
- aggregates a user's presence information from various devices using FindMe™.

Presence User Agent

- Publishes presence information on behalf of devices that are registered to the VCS, including those that do not support IETF Presence.

Scalable Deployments

A VCS can be part of a Cluster of up to six identically configured VCSs, enabling the systems to work together as one large Local Zone. This allows you to:

- increase the capacity of your VCS deployment compared with a single VCS
- provide redundancy in the rare case that a VCS becomes unavailable (for example, due to a network or power outage).

Clusters must use TMS version 12.0 and above to ensure they are configured identically.

Multiple Web Accounts

This feature allows up to 15 additional administration accounts to be created. Each administration account can be assigned either "Read Only" access, meaning they can view but not change configuration, or "Read Write" access, enabling them to modify the configuration of the VCS.

In order to track the activities of users, the VCS now also includes a Configuration Log which shows all web login attempts for administrators and Findme users (both failed and successful), and all changes to the VCS configuration made via the web UI including the name of the user who made the change.

Intelligent Route Director

The addition of Local Zone matches to the zone search process means that it is now possible to configure the VCS so that a call can be routed to a specific zone (including the Local Zone) depending on a pre-defined set of priorities and bandwidth policies. This feature enables, for example, the VCS to be configured to overflow calls from an IP zone to an ISDN gateway registered on the local zone.

H.323 version 6

TANDBERG VCS now supports H.323 version 6.

Microsoft OCS 2007 Interworking

Additional advanced zone configuration options have been included to allow calls to be made between Microsoft OCS 2007 clients and devices registered to the VCS. These options also allow Microsoft OCS clients to view basic presence information of endpoints registered to the VCS.

Backup and Restore

The Backup and Restore feature allows you to create a file containing the configuration of your VCS at a particular date and time. You can then use this file at a later date to return the VCS to that state of configuration.

Pre-Connect Transfer

To compliment support for the call forward (before and after answer) and the call hold facilities available in SIP, the VCS now interworks these supplementary services into the H.323 protocol using standards-based Facility messages.

SNMP Enhancements

The VCS now supports SNMP v2 MIB-II and Net-SNMP MIB.

Using this Administrator Guide

This Administrator Guide is provided to help you make the best use of your TANDBERG VCS.

Your approach to this documentation depends on what you want to do and how much you already know.

The Administrator Guide has been divided into several sections, each providing different information. In some places information is duplicated between sections to let you have all the relevant information in one place.

This document does not have an index. This is intentional; if the Table of Contents does not direct you to the information you need, you can use the Find function in Adobe Reader to search the text for keywords.

Note that the Administrator Guide describes a fully equipped version. Your version may not have all the described extensions installed.

Our main objective with this Guide is to address your goals and needs. Please let us know how well we succeeded!

Typographical conventions

Most configuration tasks on the VCS can be performed via either the web interface or a command line interface. This Guide will describe how to use both methods.

Web Interface

In this Guide, instructions for performing a task via the web interface are shown in the format:

- Menu > Submenu

followed by the Name of the page that you will be taken to.

In most cases a screenshot of the page will be shown adjacent, with callouts describing each of the configurable options.

Command Line Interface

In this Guide, instructions for performing a task using the command line interface (CLI) are shown in the format:

- `xConfiguration <Element> <SubElement>`
- `xCommand <Command>`

These are meant as a reference only. Each command is hyperlinked to the Command Reference table at the back of this Guide; clicking on the hyperlink will take you to the appropriate section of the table showing all the available sub-elements, parameters and valuespaces for the given command.

Note that:

- Typing the given `xConfiguration` path into the CLI will return a list of values currently configured for that element (and sub-elements where applicable).
- Typing the given `xConfiguration` path into the CLI followed by a `?` will return information about the usage for that element and sub-elements.
- Typing the given `xCommand` command into the CLI with or without a `?` will return information about the usage of that command.

Getting Started

This section describes how to install the VCS and carry out its initial configuration. It also gives an overview of the VCS's Administrator settings and describes how to access the VCS via either the Command Line Interface (CLI) or the web interface.



Installation

What's in the Box?

To avoid damage to the unit during transportation, the TANDBERG VCS is delivered in a special shipping box, which should contain the following components:

- TANDBERG VCS
- CD containing VCS Administrator Guide and other documentation
- Installation Sheet
- Registration card
- Rack ears and screws
- Cables:
  - power cables
  - ethernet cable
  - shielded serial cable

Please report any discrepancies to your TANDBERG representative immediately.



A brief yet concise description of the procedure to get you up and going can be found in the Installation Sheet accompanying your TANDBERG product.

Installation Site Preparations

- Make sure that the VCS is accessible and that all cables can be easily connected.
- For ventilation: leave a space of at least 10cm (4 inches) behind the VCS's rear panel and 10cm (4 inches) in front of the front panel.
- The room in which you install the VCS should have an ambient temperature between 0°C and 35°C (32°F and 95°F) and between 10% and 90% non-condensing relative humidity.
- Do not place heavy objects directly on top of the VCS.
- Do not place hot objects directly on top, or directly beneath the VCS.
- Use a grounded AC power outlet for the VCS.

General Installation Precautions

- The socket outlet shall be installed near to the equipment and shall be easily accessible.
- Never install cables without first switching the power OFF.

Connecting the Cables



Shielded serial cable

To control the VCS using a direct connection to a PC, connect the serial cable between the VCS's DATA port and the COM port on a PC.

Ethernet cable

To use the VCS over IP, connect the ethernet cable from the LAN1 port on the VCS to your network.

The LAN2 port can also be used if you have the Dual Network Interfaces option installed.

The LAN3 and LAN4 ports are not used.



Power switch

Soft power button

Power cable

Connect the system power cable to an electrical distribution socket.

Initial Configuration

Powering on the VCS

To start the VCS:

1. Ensure the power cable is connected.
2. Ensure the LAN cable is connected to the LAN1 port.
3. Turn on the power switch on the back right of the unit (adjacent to the power cable).
4. Press the soft power button on the back left of the unit.

The system will power up. Wait until:

- the green PWR LED on the front of the unit is a steady green color (it may flash briefly during power up).
- the red ALM LED on the front of the unit has gone out.
- the IP address is showing in the display panel on the front of the unit.

You now must set the system's IP address, subnet mask and default gateway before the system can be used. Consult your network administrator for information on which addresses to use. Note that the VCS must use a static IP address.

The initial configuration can be done:

- by connecting from a PC to the VCS via a serial cable
- via the buttons on the front panel
- if your network is set up to allow it, by connecting via a web browser to the default IP address of 192.168.0.100.

If the red ALM LED flashes rapidly it indicates a hardware fault. Contact your local TANDBERG representative.

The yellow HDD LED indicates disk activity and may flicker during normal operation, more so on a busy system.

Initial Configuration via Serial Cable

To set the initial configuration using a PC connected to the VCS DATA port via a serial cable:

1. Connect the supplied serial cable from the DATA port on the VCS to the COM port on a PC.
2. Start a terminal emulator program on the PC and configure it to use the DATA port as follows:
   - baud rate 115200
   - data bits: 8
   - parity: none
   - stop bits: 1
   - flow control: none.
3. Power on the unit (if it is not already on).

   The terminal emulator program will display start up information.

   After approximately 2 minutes you will get the login prompt (if the unit is already on, press Enter to get the login prompt):

   `tandberg login:`
4. Enter the username admin and press Enter. You will get the password prompt: `Password:`
5. Enter the default password of TANDBERG and press Enter.

   You will get the install wizard prompt:

   `Run install wizard [n]:`

   Type `y` and press Enter.
6. Follow the prompts given by the install wizard to specify the following:

   a. The password you want to use for your admin account. See Default Administrator Account for details.

   b. Whether you wish to use IPv4, IPv6 or Both. See IP Protocol for details.

   c. The LAN1 IP address of the system.

   d. The LAN1 IPv4 subnet mask of the system (if you have selected IPv4).

   e. The IP default gateway of the system.

   f. The ethernet speed.

   g. Whether you want to use SSH to administer the system.

   h. Whether you want to use Telnet to administer the system.
7. Once the wizard is finished you will be prompted to log in again. Login with the username admin and your new password.
8. You will again get the install wizard prompt; this time select `n` and press Enter in order to skip the wizard.

   A welcome message similar to the following will appear:

   ```
   Welcome to
   TANDBERG VCS Release X3.0
   SW Release Date: 2008-07-01
   OK
   ```
9. You must now reboot the system in order for the new settings take effect. To do this, type the command:
   - `xCommand boot`

Once it has rebooted, the VCS is ready to use. You can continue to use the serial connection, or you can connect to the system remotely over IP using either or both:

- the web interface via HTTPS
- a command line interface via SSH or Telnet.

We recommend that you now configure the following:

- The system name of the VCS. This is used by the TANDBERG Management Suite (TMS) to identify the system. See About the System Name for more information.
- Automatic discovery. If you have multiple VCSs in the same network you may want to disable automatic discovery on some of them. See Auto Discover for more information.
- The DNS server address (if URI dialing or FQDNs are to be used). See DNS configuration for more information.

The IP configuration made via the serial cable applies to the LAN 1 ethernet port only. If you have enabled the LAN 2 port (by installing the Dual Network Interfaces option key) you must use the web interface or CLI to configure the LAN 2 settings.

Do not leave a terminal emulator session open once it is no longer in use. An open session may cause issues during a system restart.

Initial Configuration

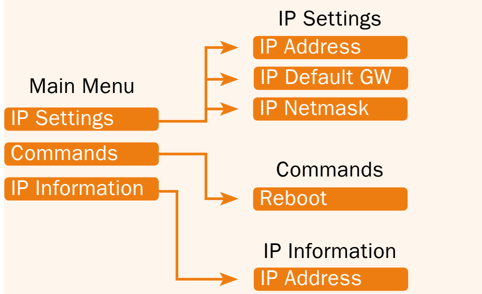
Initial Configuration via Front Panel

The LCD panel makes it possible to configure and check the IP settings as well as to reboot the system.

By default, during normal operation the front panel will show the system name (if configured) and the LAN 1 IPv4 Address.

To access the front panel menu options, press ENTER.

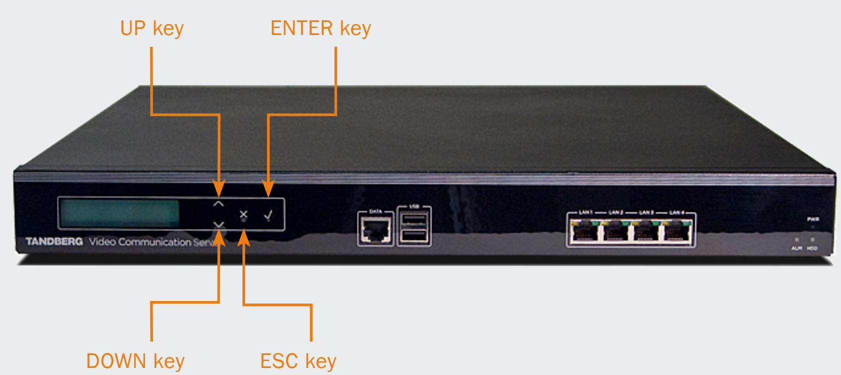
The front panel LCD menu items are as follows:



The steps opposite give an example of how to use the front panel, in this case to configure the LAN 1 IPv4 address. Use the same procedure to configure the system's LAN 1 IPv4 subnet mask and IPv4 default gateway.

The IPv4 address and IPv4 subnet mask configuration made via the front panel applies to the LAN 1 ethernet port only. To configure the system's IPv6 settings and (if you have the Dual Network Interfaces option key installed) the LAN 2 settings, you must use the web interface or CLI.

1. Press ENTER to produce the Main Menu. Use UP/DOWN to navigate to the IP Settings submenu.
2. Press ENTER to access the IP Settings submenu.
3. Use the UP/DOWN keys to navigate to IP Address and press ENTER to select this option.
4. Press ENTER again to produce the cursor.
5. Use the UP/DOWN keys to move left and right between the digits of the number.
6. When you reach a digit you wish to change, press ENTER.
7. Use UP/DOWN to increase or decrease the digit value. Press ENTER to select the amended digit.
8. To amend the remaining digits, either press ENTER to move to the right, or ESC followed by UP/DOWN to move to the left.
9. When you have finished editing press ESC twice to go to the Confirm change menu.
10. Use the UP/DOWN key to select yes or no followed by ENTER to confirm.
11. Use ESC key to navigate back to the main menu.
12. Repeat the process, selecting IP Default GW to configure the default gateway and IP Netmask for the subnet mask.



System Administrator Access

Overview

About Administrator Access

While it is possible to administer the TANDBERG VCS via a PC connected directly to the unit via a serial cable, you may wish to access the system remotely over IP.

You can do this using either or both:

- the web interface via HTTPS
- a command line interface (CLI) via SSH or Telnet.

By default, access via HTTPS and SSH is enabled; access via Telnet is disabled. These can be enabled and disabled according to your requirements.

You can also enable access via HTTP. However, this mode works by redirecting HTTP calls to the HTTPS port, so HTTPS must be enabled for access via HTTP.

Tandberg Management Suite (TMS) accesses the VCS via the web server. If HTTPS mode is turned off, TMS will not be able to access it.

Configuring Administrator Access

To configure the ways in which your system is accessed:

- System Configuration > System.
  You will be taken to the System Administration page.
  In the Admin Access section, select Off or On from the drop-down boxes for each service.
- `xConfiguration Administration`

You must restart the system for any changes to the Administrator settings to take effect.

Administration Accounts

The VCS has a default administrator account with full read/write access. This account is used to log into the VCS via the web UI or the CLI. You can add additional administrator accounts with either read/write access or read-only access; these can be used to log in via the web UI only. See the Administration Accounts section for information on how to create these additional accounts.

Default Administrator Account

The default administrator account has a username of admin (all lower case) and a default password of TANDBERG (all upper case). You cannot delete the default administrator account or change the admin username, but you should change the password as soon as possible. Choose a strong password, particularly if administration over IP is enabled.

Changing the Default Administrator Password

To change the administrator password:

- Maintenance > Administration Accounts.
  You will be taken to the Administration Accounts page.
  Click on View/Edit for the admin name.
  You will be taken to the Edit Administration Account page.
  In the Password and Confirm Password fields, enter the new password, and click Save.

  To set an empty password via the web UI, delete the characters from the Password and Confirm Password fields and click Save.
- `xConfiguration SystemUnit Password`

  To set an empty password via the CLI, type:
  `xConfiguration SystemUnit Password: ""`

Resetting the Default Administrator Password

If you forget your password, it is possible to set a new password using the following procedure:

1. Connect a PC to the VCS using the serial cable as per the instructions in steps 1 and 2 of Initial Configuration via Serial Cable.
2. Reboot the VCS.
3. Login from the PC with the username pwrec. No password is required.
4. You will be prompted for a new password.

The pwrec account is only active for one minute following a restart. Beyond that time you will have to restart the system again to change the password.

It is possible to have more than one Administrator session running at the same time. These sessions could be via the web interface, command line interface, or a mixture of both. This may cause issues if each Administrator session is attempting to make the same configuration changes.

Root Account

The VCS provides a root account which will have the same password as the admin account. The root account should not be used in normal operation, and in particular system configuration should not be conducted using this account. Use the admin account instead.

Administrator Session Timeout

By default, Administrator sessions do not time out – they remain active until you logout.

You can set the system to timeout an Administrator session after a set number of minutes of inactivity. The timeout period will apply to all Administrator sessions using both the Web Interface and the Command Line Interface.

To set the timeout period:

- System Configuration > System.
  You will be taken to the System Administration page.
  In the Admin Access section, in the Session time out (minutes) box, enter the number of minutes of inactivity after which an administrator session should time out.
- `xConfiguration Administration TimeOut`

Values must be between `0` and `10,000`. A value of `0` means that Administrator sessions will never time out.

Security Considerations

To securely manage the VCS you should disable Telnet, using the encrypted HTTPS and SSH protocols instead. For further security, disable HTTPS and SSH as well and use the serial port to manage the system.

Because access to the serial port allows the password to be reset, it is recommended that you install the VCS in a physically secure environment.

Web Interface

Using the Web Interface

To use the web interface:

1. Open a browser window and in the address line type either:
   - the IP address of the system
   - the FQDN of the system.
2. Select Administrator Login.
3. Enter a valid administration username and password and select Login.

You will be presented with the Overview page.

When logging in via the VCS web interface, you may receive a warning message regarding the VCS's security certificate. This can safely be ignored.

Supported Browsers

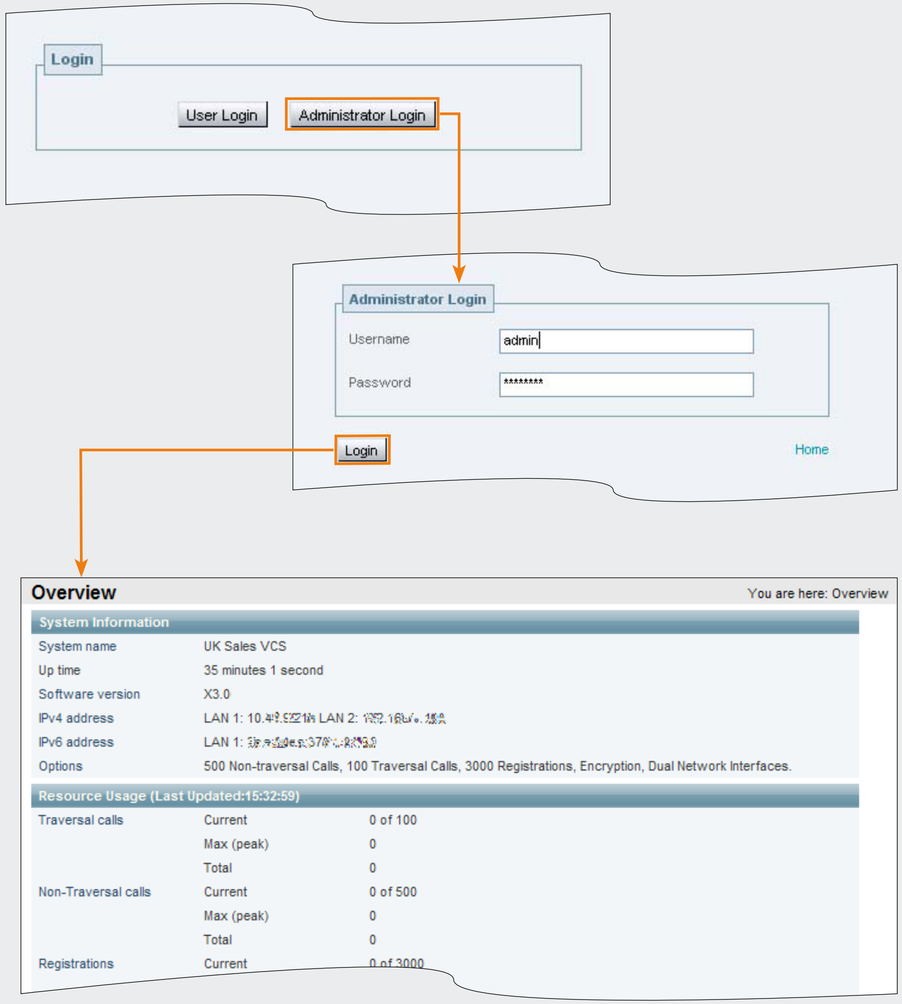
The VCS web interface is designed for use with Internet Explorer (6 and up) or Firefox (1.5 and up). It may work with Opera and Safari, but you may encounter unexpected behavior.

Javascript and cookies must be enabled to use the VCS web interface.

In this Administrator Guide, instructions for performing a task via the web interface are shown in the format:

- Menu option1 > Menu option2

followed by the Name of the page that you will be taken to in order to perform the task. In most cases the page will be shown adjacent with callouts describing each of the configurable options.



System Administrator Access

Web Interface

General page features

These are the features that can be found on some or all of the web UI pages.

Note that you will not be able to change settings if your admin account is read only.

Information bar

The VCS provides you with feedback in certain situations, for example when settings have been saved or when you need to take further action. This feedback is given in a yellow information bar at the top of the page.

Sorting Columns

Click on column headings to sort the information in ascending and descending order.

Select All and Unselect All

Use these buttons to select and unselect all items in the list.

Status

On configuration pages, this section shows you the current status of the items you are configuring.

Note that some configuration requires a reboot to take effect, so if you have changed the configuration but not yet rebooted this will show the existing (unchanged) status.

System Information

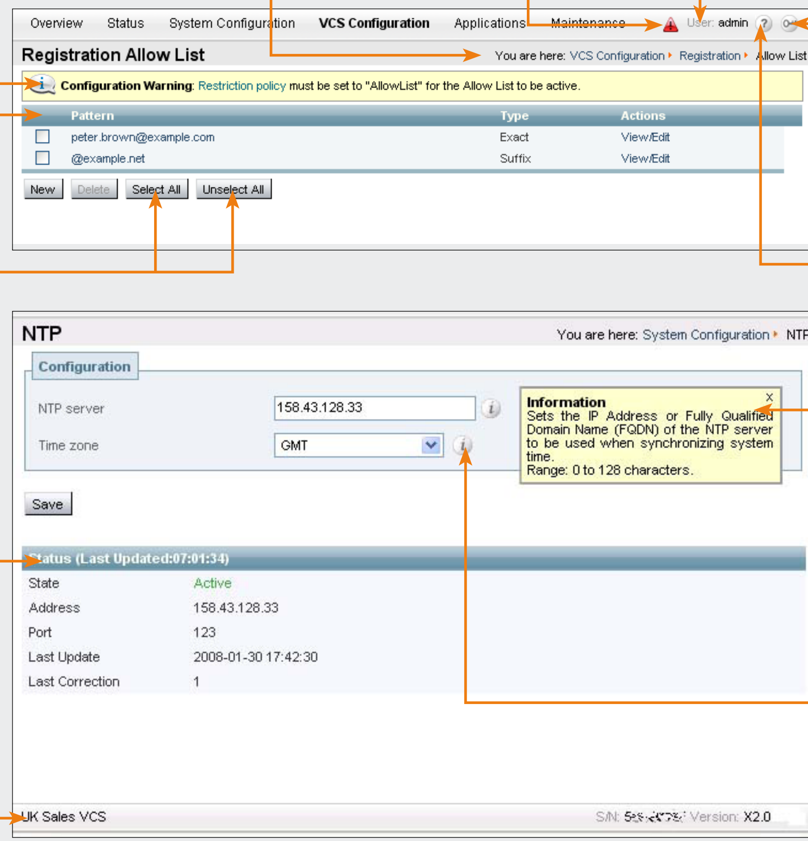
Each page will always show the system name (or LAN 1 IPv4 address if no system name is configured) at the bottom left corner, and the hardware serial number and VCS software version at the bottom right corner.

Page name and Location

Every page shows the page name and the menu path that you took to get there. Each part of the menu path is a link; clicking on any of the higher level menu items will take you to that page.

System Warning

This icon appears on the top right corner of every page when there is a system warning in place. Click on this icon to go to the Warnings page which gives information about the warning and its suggested resolution.



User

The username of the administration account used to log in to the VCS.

Log out

This icon appears on the top right corner of every page. Clicking on this icon will end your Administrator session. You will be taken to the Administrator Login page.

View manual

This icon appears on the top right corner of every page. Clicking on this icon will take you directly to the latest version of the VCS Administrator Guide on the TANDBERG website.

Information box

A yellow information box will appear on the configuration pages whenever you either click on the Information icon or click inside a field. This box gives you information about the particular field, including where applicable the valid ranges and default value.

To close the information box, click on the X at its top right corner.

Information

This icon appears to the right of most input fields in the web interface.

Clicking on this icon will activate the Information Box.

System Administrator Access

Command Line Interface

Using the Command Line Interface (CLI)

The command line interface is available over SSH, Telnet and through the serial port.

To use the command line interface:

1. Start a SSH or Telnet session.
2. Enter the IP address or FQDN of the VCS.
3. Login with a username of admin and your system password.

You will see a screen similar to that shown on the right. You are now ready to start using the CLI by typing the appropriate commands.

Types of Commands

Commands are divided into different groups according to their function:

xStatus	These commands return information about the current status of the system. Information such as current calls and registrations is available through this command group.
xConfiguration	These commands allow you to add and edit single items of data such as IP address and zones.
xCommand	These commands allow you to add and configure items and obtain information.
xHistory	These commands provide historical information about calls and registrations.
xFeedback	These commands provide information about events as they happen, such as calls and registrations.

See the Command Reference Appendix for a full description of commands available on the VCS.

How Command are Shown in this Guide

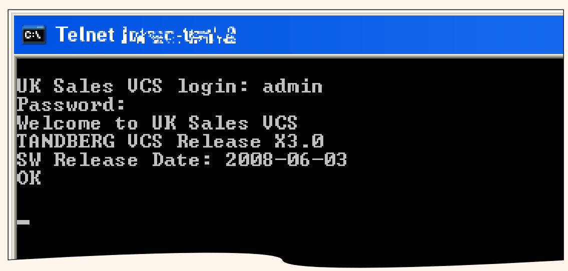
In this Guide, instructions for performing a task using the command line interface (CLI) are shown in the format:

- xConfiguration <Element> <SubElement>
- xCommand <Command>

These are meant as a reference only. Each command is hyperlinked to the Command Reference table at the back of this Guide; clicking on the hyperlink will take you to the appropriate section of the table showing all the available sub-elements, parameters and valuespaces for the given command.

Note that:

- Typing the given xConfiguration path into the CLI will return a list of values currently configured for that element (and sub-elements where applicable).
- Typing the given xConfiguration path into the CLI followed by a ? will return information about the usage for that element and sub-elements.
- Typing the given xCommand command into the CLI with or without a ? will return information about the usage of that command.



Supported Characters

The VCS supports the following characters when entering text in the CLI and web UI:

- the letters A-Z and a-z
- decimal digits (0-9)
- underscore (_)
- minus sign (-)
- equals sign (=)
- plus sign (+)
- at sign (@)
- comma (,)
- period/full stop (.)
- exclamation mark (!)
- spaces

The following characters are specifically not allowed:

- tabs
- angle brackets (< and >)
- ampersand (&)
- caret (^)

Overview and Status

This section describes the information that appears on the Overview page and all the pages under the Status menu of the web interface.

These pages provide information on the current status and configuration of the VCS.



Overview

Viewing the Overview Page

The Overview page summarizes the current configuration and status of your VCS.

The Overview page opens automatically when you first log on to the web interface.

You can also access it at any time by clicking on the Overview menu at the top left of any page.

System name

The name that has been assigned to the VCS.

Up time

The amount of time that has elapsed since the system last restarted.

Software version

The version of software that is currently installed on the VCS.

IPv4 address

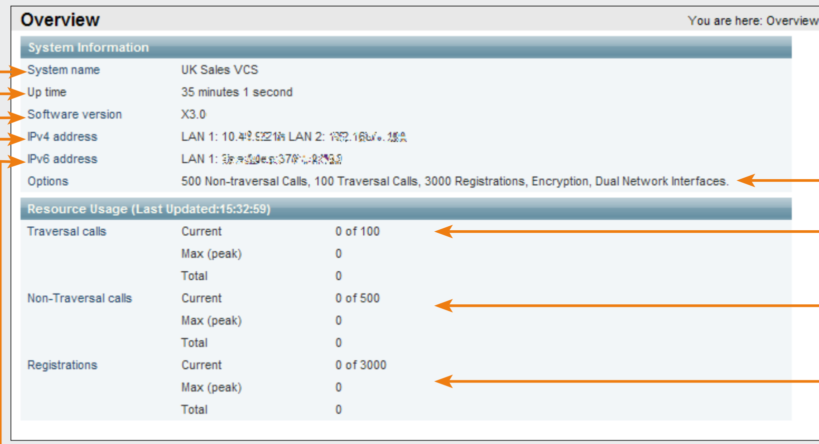
The VCS's IPv4 address(es).

IPv6 address

The VCS's IPv6 address(es).

Many of the items on this page are configurable, and contain links to the page where they can be configured. For example, clicking on System name will take you to the System Administration page, from where you can configure the system name.

Understanding the Overview Page



Options

The maximum number of calls and registrations, and the availability of additional VCS features such as User Policy and Dual Network Interfaces, are controlled through the use of Option Keys. This section shows all the Options that are currently installed on the VCS.

Traversal calls

Current: The number of traversal calls going through the VCS at this moment.

Max (peak): The highest number of concurrent traversal calls handled by the VCS since it was last restarted.

Total: The total number of traversal calls handled by the VCS since it was last restarted.

See the section Traversal Calls for details on what constitutes a traversal call.

Non-traversal calls

Current: The number of non-traversal calls going through the VCS at this moment.

Max (peak): The highest number of concurrent non-traversal calls handled by the VCS since it was last restarted.

Total: The total number of non-traversal calls handled by the VCS since it was last restarted.

Registrations

Current: The number of endpoints registered to the VCS at this moment.

Max (peak): The highest number of endpoints concurrently registered to the VCS since it was last restarted.

Total: The total number of registrations on the VCS since it was last restarted.

System Information

Viewing the System Information Page

The System Information page provides details of the software, hardware, and time settings of the VCS.

To view the System Information page:

- Status > System > Information

Up time

The amount of time that has elapsed since the system last restarted.

System time (UTC)

The time as determined by the NTP server.

If no NTP server has been configured, this will show Time Not Set.

Time zone

The time zone that has been configured on the NTP page.

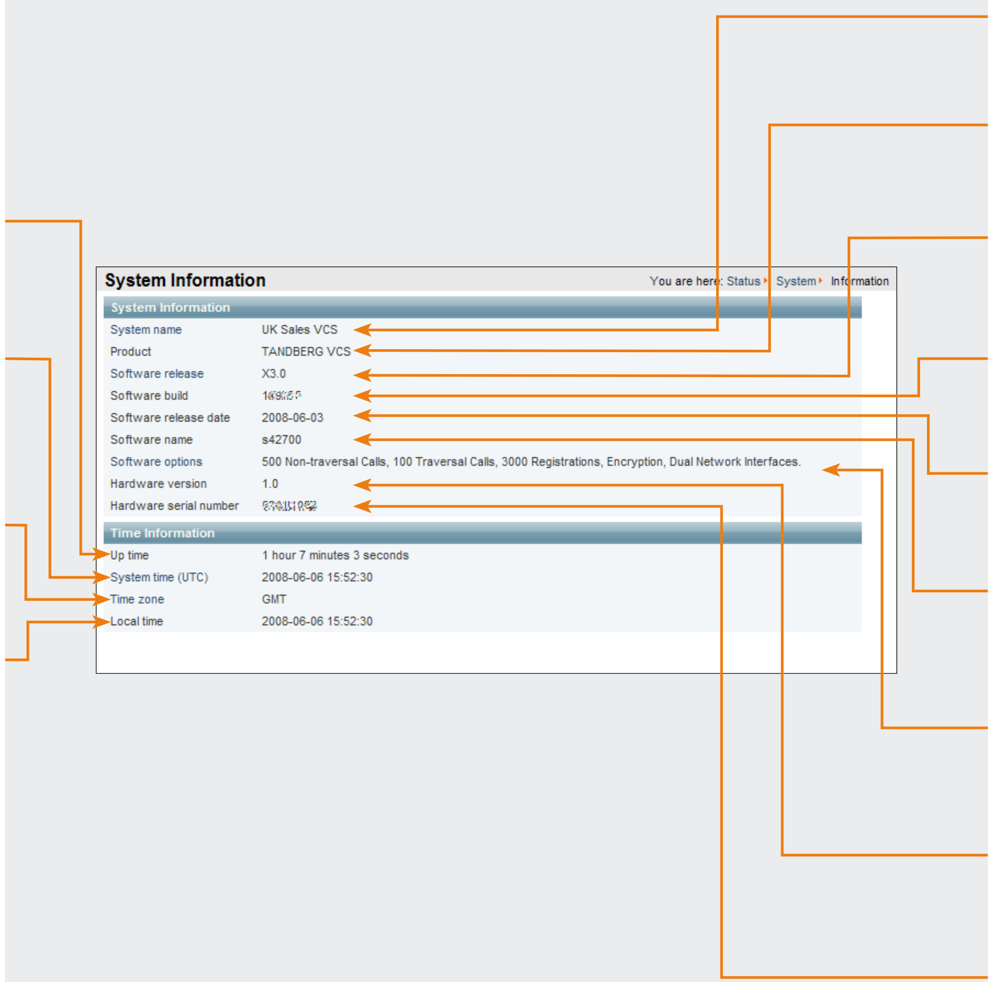
Local time

If an NTP server has been configured, this will be a combination of the NTP server time (which is UTC) and the local time zone.

If no NTP server has been configured, this will show the time according to the VCS's operating system.

Some of the items on this page are configurable, and contain links to the page where they can be configured. For example, clicking on Software Options will take you to the Option Keys page, from where you can install new optional features.

Understanding the System Information Page



System name

The name that has been assigned to the VCS.

Product

This will be TANDBERG VCS.

Software release

The version of software that is currently installed on the VCS.

Software build

The build number of this software version.

Software release date

The date on which this version of the software was released.

Software name

The internal TANDBERG reference number for this software release.

Software options

All the extra features installed on the VCS via option keys.

Hardware version

The version number of the hardware on which the VCS software is installed.

Hardware serial number

The serial number of the hardware on which the VCS software is installed.

Ethernet

Viewing the Ethernet Status Page

The Ethernet page provides details of the MAC address and ethernet speed settings of the VCS.

To view the Ethernet page:

- Status > System > Ethernet

Understanding the Ethernet Status Page



MAC address

The MAC address of the VCS's ethernet device.

If the Dual Network Interfaces option key has been installed, this will show the MAC addresses of the ethernet cards for both the LAN1 port and the LAN2 port.

Speed

The speed of the connection between the VCS and the ethernet switch.

If the Dual Network Interfaces option key has been installed, this will show the ethernet speed for both the LAN1 port and the LAN2 port.

IP Status

Viewing the IP Status Page

The IP Status page provides details of the IP and DNS settings of the VCS.

To view the IP Status page:

- Status > System > IP

Protocol

Indicates the IP protocol supported by the VCS.

IPv4: The VCS will only accept registrations from endpoints using an IPv4 address, and will only take calls between two endpoints or devices communicating via IPv4. It will communicate with other systems via IPv4 only.

IPv6: The VCS will only accept registrations from endpoints using an IPv6 address, and will only take calls between two endpoints communicating via IPv6. It will communicate with other systems via IPv6 only.

Both: The VCS will accept registrations from endpoints using either an IPv4 or IPv6 address, and will take calls using either protocol. If a call is between an IPv4-only and an IPv6-only endpoint, the VCS will act as an IPv4 to IPv6 gateway (note that this will require a traversal call licence). The VCS can communicate with other systems via either protocol.

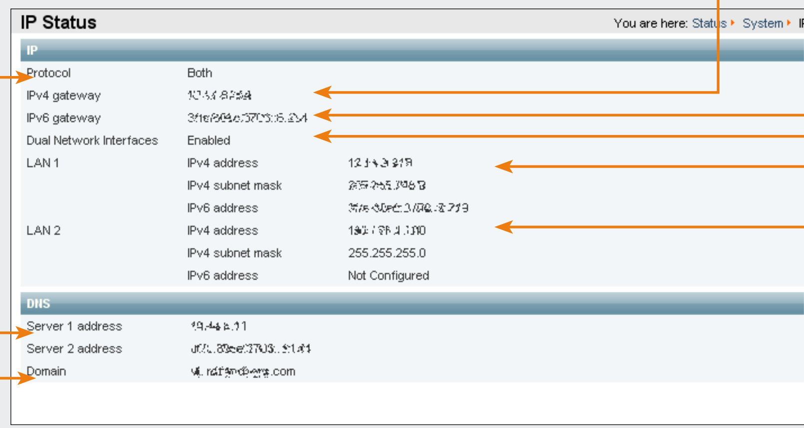
Server 1..5 address

The IP address(es) of each of the DNS servers that will be queried when resolving domain names. Up to 5 DNS servers may be configured.

Domain

Specifies the name to be appended to the host name before a query to the DNS server is executed.

Understanding the IP Status Page



IPv4 gateway

The IPv4 gateway used by VCS.

IPv6 gateway

The IPv6 gateway used by VCS.

Dual Network Interfaces

Indicates whether the second LAN port has been enabled. This is done by installing the Dual Network Interfaces option key.

LAN 1

Shows the IPv4 Address and subnet mask, and IPv6 Address of the LAN1 port.

LAN 2

If the Dual Network Interfaces option key has been installed, this shows the IPv4 Address and subnet mask, and IPv6 Address of the LAN2 port.

Resource Usage

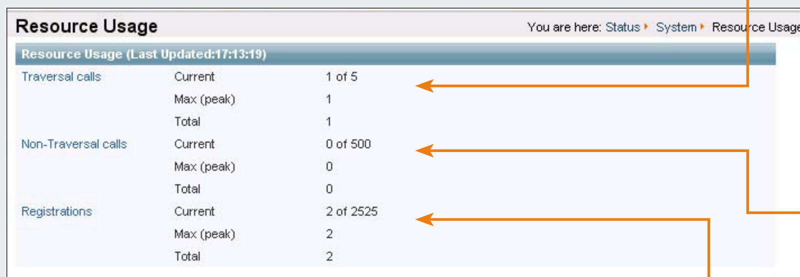
Viewing the Resource Usage Page

The Resource Usage page provides statistics about the numbers of current and cumulative calls and registrations on the VCS. This page automatically refreshes every 5 seconds.

To view the Resource Usage page:

- Status > System > Resource Usage

Understanding the Resource Usage Page



Traversal calls

Current: The number of traversal calls going through the VCS at this moment.

Max (peak): The highest number of concurrent traversal calls handled by the VCS since it was last restarted.

Total: The total number of traversal calls handled by the VCS since it was last restarted.

Non-traversal calls

Current: The number of non-traversal calls going through the VCS at this moment.

Max (peak): The highest number of concurrent non-traversal calls handled by the VCS since it was last restarted.

Total: The total number of non-traversal calls handled by the VCS since it was last restarted.

Registrations

Current: The number of devices registered to the VCS at this moment.

Max (peak): The highest number of devices concurrently registered to the VCS since it was last restarted.

Total: The total number of registrations on the VCS since it was last restarted.

Registrations

Viewing the Registrations Page

The Registrations page lists all the devices that are currently registered with the VCS.

Devices that are configured for both SIP and H.323 will register twice; once as an H.323 endpoint and once as a SIP UA.

To view the Registrations page:

- Status > Registrations

Unregister

Click here to remove the selected registrations.

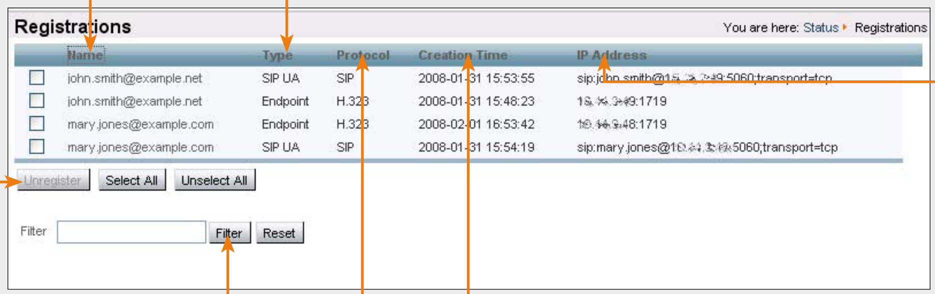
Note that removing a registration will not prevent the same device from automatically re-registering.

Filter

To limit the list of registrations, enter one or more characters in the Filter field and select Filter. Only those registrations that contain (in any of the displayed fields) the string you entered will be shown.

To return to the full list of registrations, click Reset.

Understanding the Registrations Page



Name

The H.323 alias or SIP AOR that the device registered.

Clicking on an individual name will take you to the Registrations Details page for that registration.

Type

Indicates the nature of the registration. This will most commonly be Endpoint, Gateway, or SIP UA.

IP Address

For H.323 devices, this is the RAS address.

For SIP UAs it is the Contact address presented in the REGISTER request.

Creation Time

The date and time at which the registration was accepted.

If an NTP server has not been configured, this will say Time not set.

Protocol

Whether the registration is for a SIP or H.323 device.

Registration History

Viewing the Registration History Page

The Registration History page lists all the registrations that are no longer current. It lists the most recent historical registrations since the last reboot, up to a maximum of 255.

To view the Registration History page:

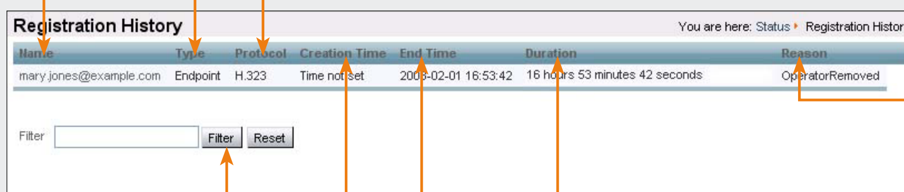
- Status > Registration History

Filter

To limit the list of registrations, enter one or more characters in the Filter field and select Filter. Only those registrations that contain (in any of the displayed fields) the string you entered will be shown.

To return to the full list of registrations, click Reset.

Understanding the Registration History Page



Name

The H.323 alias or SIP AOR that the device registered.

Clicking on an individual name will take you to the Registrations Details page for that registration.

Type

Indicates the nature of the registration. This will most commonly be Endpoint, Gateway, or SIP UA.

Protocol

Whether the registration was for a SIP or H.323 device.

Reason

The reason why the registration was terminated.

Duration

The length of time that the registration was in place.

End Time

The date and time at which the registration was terminated.

Creation Time

The date and time at which the registration was accepted.

If an NTP server has not been configured, this will say Time not set.

Viewing the Presence Status Pages

The Status > Presence menu has three sub-menus:

- Publishers
- Presentities
- Subscribers.

These pages provide information about endpoints and presentities using the Presence services on the VCS.

Refer to the Viewing Presence Status section for a full explanation of the information on these pages.

Viewing the Calls Page

The Calls page lists all the calls currently taking place to or from devices registered with the VCS, or that are passing through the VCS.

To view the Calls page:

- Status > Calls

Disconnect

Click here to disconnect the selected calls.

Call disconnection works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, and interworked H.323 to SIP calls, the Disconnect command will actually disconnect the call.

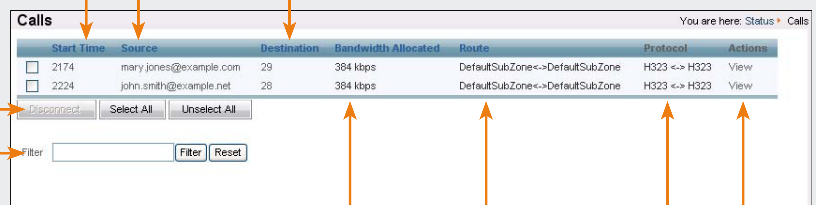
For SIP to SIP calls, the Disconnect command will cause the VCS to release all resources used for the call and the call will appear on the system as disconnected. However, SIP calls are peer-to-peer and as a SIP proxy the VCS has no authority over the endpoints. Although releasing the resources may have the side-effect of disconnecting the SIP call, it is also possible that the call signaling, media or both may stay up (depending on the type of call being made). The call will not actually disconnect until the SIP endpoints involved have also cleared their resources.

Filter

To limit the list of calls, enter one or more characters in the Filter field and select Filter. Only those calls that contain (in any of the displayed fields) the characters you entered will be shown.

To return to the full list of calls, click Reset.

Understanding the Calls Page



Start time

The date and time at which the call was placed.

Source

The alias of the device that placed the call.

Destination

The alias to which the call was placed.

This may be different from the alias that was actually dialed from the device, as it may have been transformed either locally or before the zone was queried.

Actions

Click View to go to the Call Details page which lists full details of this call.

Protocol

Shows whether the call used H.323, SIP, or both protocols.

Route

The subzone or zone from which the call was received and the subzone or zone to which the call was placed.

Intermediary subzones are not shown here. To see the complete route within the VCS that the call took, click on View to go to the Call Details page.

Bandwidth Allocated

The amount of bandwidth allocated to this call.

Call History

Viewing the Call History Page

The Call History page lists all the calls that are no longer active that have taken place since the VCS was last restarted.

To view the Call History page:

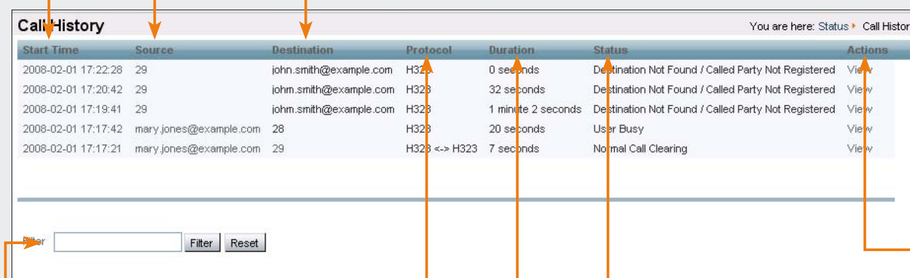
- Status > Call History

Filter

To limit the list of calls, enter one or more characters in the Filter field and select Filter. Only those calls that contain (in any of the displayed fields) the characters you entered will be shown.

To return to the full list of calls, click Reset.

Understanding the Call History Page



Start time

The date and time at which the call was placed.

Source

The alias of the device that placed the call.

Destination

The alias to which the call was placed.

This may be different to the alias that was actually dialed from the endpoint, as it may have been transformed either locally or before the zone was queried.

Actions

Click View to go to the Call Details page which lists full details of this call.

Status

The reason the call was terminated.

Duration

The length of time of the call.

Protocol

Shows whether the call used H.323, SIP, or both protocols.

Search History

Viewing the Search History Page

The Search History page lists all the searches that have taken place since the VCS was last restarted.

To view the Search History page:

- Status > Search History

About Searches

For H.323, two messages are sent for every call that is placed locally: the first is an ARQ which locates the device being called, and the second is the call setup which sends a request to the device asking it to accept the call. Each message shows up as a separate search in the Search History page, but only the Setup message will be associated with a particular call.

For H.323 searches originating from external zones, an LRQ will appear in the search history.

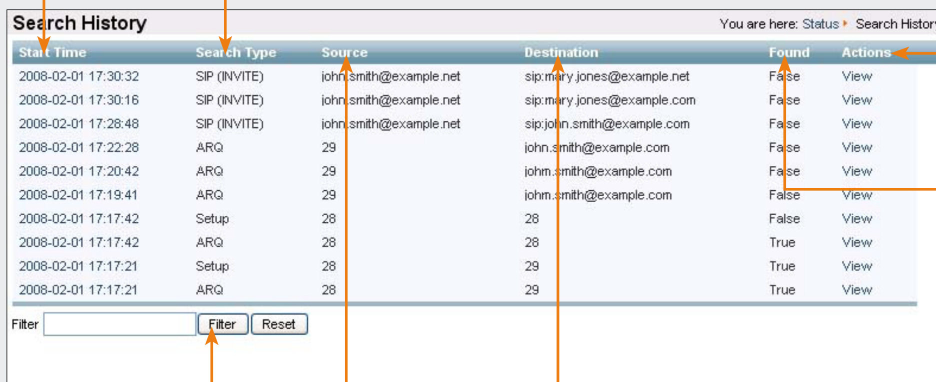
For SIP, a single message is sent in order to place a call: this is the SIP INVITE.

Filter

To limit the list of calls, enter one or more characters in the Filter field and select Filter. Only those calls that contain (in any of the displayed fields) the characters you entered will be shown.

To return to the full list of calls, click Reset.

Understanding the Search History Page



Search History — You are here: Status ▸ Search History

Start Time	Search Type	Source	Destination	Found	Actions
2008-02-01 17:30:32	SIP (INVITE)	john.smith@example.net	sip:mary.jones@example.net	False	View
2008-02-01 17:30:16	SIP (INVITE)	john.smith@example.net	sip:mary.jones@example.com	False	View
2008-02-01 17:28:48	SIP (INVITE)	john.smith@example.net	sip:john.smith@example.com	False	View
2008-02-01 17:22:28	ARQ	29	john.smith@example.com	False	View
2008-02-01 17:20:42	ARQ	29	johm.smith@example.com	False	View
2008-02-01 17:19:41	ARQ	29	johm.smith@example.com	False	View
2008-02-01 17:17:42	Setup	28	28	False	View
2008-02-01 17:17:42	ARQ	28	28	True	View
2008-02-01 17:17:21	Setup	28	29	True	View
2008-02-01 17:17:21	ARQ	28	29	True	View

Filter [Filter] [Reset]

Start time

The date and time at which the search was initiated.

Search Type

The type of message being sent.

Actions

Click View to go to the Search Details page which lists full details of this call.

Found

Indicates whether or not the search was successful.

True: the search was successful.

False: the search was unsuccessful.

Destination

The alias that was dialed from the endpoint.

This may be different from the alias to which the call was actually placed, as the original alias may have been transformed either locally or before the neighbor was queried.

Source

The alias of the endpoint that initiated the call.

Local Zone

Viewing the Local Zone Page

The Local Zone page lists all the subzones that together make up the Local Zone. This will always include the Default Subzone and the Traversal Subzone, plus any other subzones that you have created.

To view the Local Zone page:

- Status > Local Zone

Each subzone name is also a link to the configuration page for that subzone. To configure the subzone, click on the subzone name.

Understanding the Local Zone Page



Subzone Name

The names of each subzone currently configured on this VCS.

Registrations

The number of devices currently registered within each subzone.

Note that devices cannot be registered to the Traversal Subzone.

Bandwidth Used

The total amount of bandwidth used by all calls passing through each subzone.

Calls

The number of calls currently passing through each subzone.

Note that a single call may pass through more than one subzone, depending on the route it takes. For example, traversal calls from a locally registered endpoint will always pass through the Traversal Subzone, so they will show up twice; once in the originating subzone and once in the Traversal Subzone.

Viewing the Zones Page

The Zones status page lists all the zones that are currently configured on your VCS, the number of calls and amount of bandwidth being used by each, and their current status.

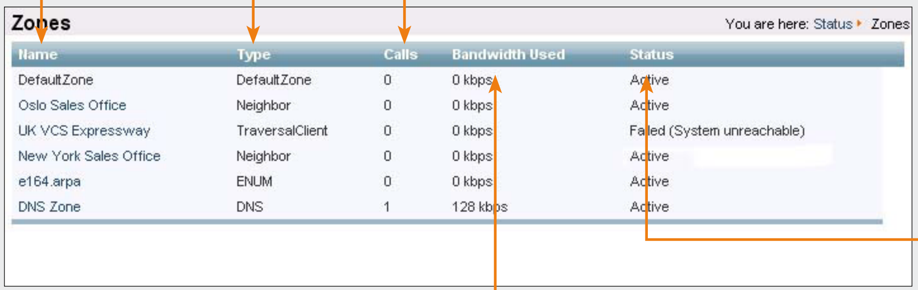
The list of zones will always include the Default Zone, plus any other zones that you have created.

To view the Zones page:

- Status > Zones

Each zone name is also a link to the configuration page for that zone. To configure the zone, click on the zone name. Note that this does not apply to the Default Zone, as this is not configurable.

Understanding the Zones Page



Name

The names of each zone currently configured on this VCS.

Type

The type of zone.

See About Zones for a full description of each zone type.

Calls

The number of calls currently passing out to or received in from each zone.

Status

The current status of each zone.

Bandwidth Used

The total amount of bandwidth used by all calls passing out to or received in from each zone.

Links

Viewing the Links Page

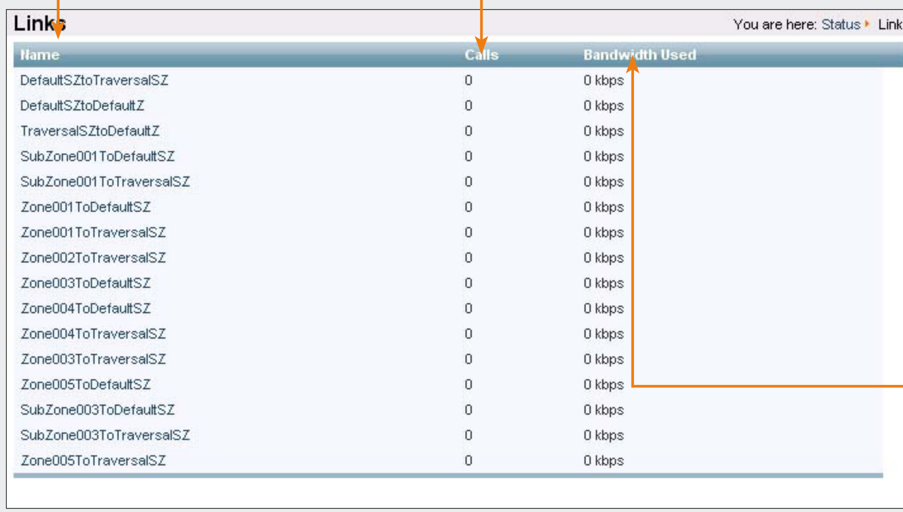
The Links status page gives you an overview of all the links currently configured on your VCS, along with the number of calls and the bandwidth being used by each link.

To view the Links status page:

- Status > Links

Each link name is also a hyperlink to the configuration page for that link. To configure the link, click on the link name.

Understanding the Links Page


Links
You are here: Status ▸ Links

Name	Calls	Bandwidth Used
DefaultSZtoTraversalSZ	0	0 kbps
DefaultSZtoDefaultZ	0	0 kbps
TraversalSZtoDefaultZ	0	0 kbps
SubZone001ToDefaultSZ	0	0 kbps
SubZone001ToTraversalSZ	0	0 kbps
Zone001ToDefaultSZ	0	0 kbps
Zone001ToTraversalSZ	0	0 kbps
Zone002ToTraversalSZ	0	0 kbps
Zone003ToDefaultSZ	0	0 kbps
Zone004ToDefaultSZ	0	0 kbps
Zone004ToTraversalSZ	0	0 kbps
Zone003ToTraversalSZ	0	0 kbps
Zone005ToDefaultSZ	0	0 kbps
SubZone003ToDefaultSZ	0	0 kbps
SubZone003ToTraversalSZ	0	0 kbps
Zone005ToTraversalSZ	0	0 kbps

Name

The name of each link.

Calls

The total number of calls currently traversing each link. Note that a single call may traverse more than one link, depending on how your system is configured.

Bandwidth Used

The total bandwidth of all the calls currently traversing each link.

Pipes

Viewing the Pipes Page

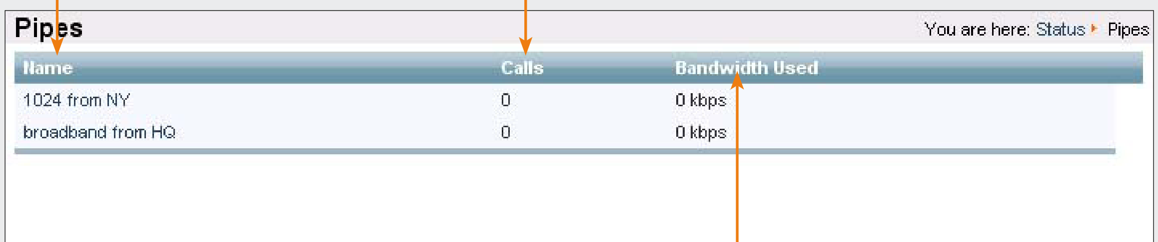
The Pipes page provides a list of all the pipes currently configured on your VCS, along with the number of calls and the bandwidth being used by each pipe.

To view the Pipes status page:

- Status > Pipes

Each pipe name is also a link to the configuration page for that pipe. To configure the pipe, click on the pipe name.

Understanding the Pipes Page



Name

The name of each pipe.

Clicking on the name will take you to the Edit Pipe page, where you can configure the pipe.

Calls

The number of calls currently traversing each pipe.

Note that a single call may traverse more than one pipe, depending on how your system is configured.

Bandwidth Used

The total bandwidth of all the calls currently traversing each pipe.

STUN Relays

Viewing the STUN Relays Page

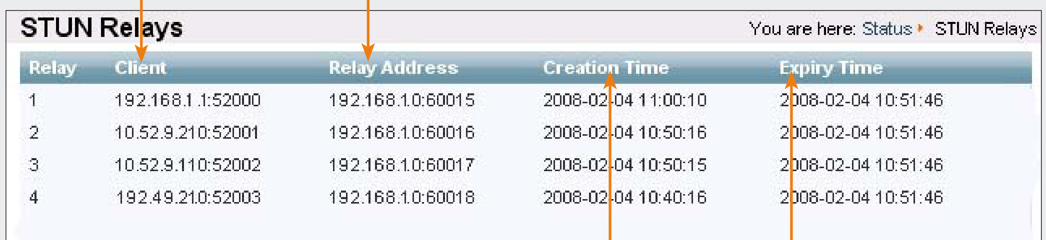
The STUN Relays page provides a list of all the currently active STUN Relays on the VCS. For each Relay, it shows the requesting client address and port and the corresponding VCS address and port.

To view the STUN Relays page:

- Status > STUN Relays

STUN services are available on VCS Expressways only.

Understanding the STUN Relays Page


STUN Relays

You are here: Status ▸ STUN Relays

Relay	Client	Relay Address	Creation Time	Expiry Time
1	192.168.1.1:52000	192.168.1.0:60015	2008-02-04 11:00:10	2008-02-04 10:51:46
2	10.52.9.210:52001	192.168.1.0:60016	2008-02-04 10:50:16	2008-02-04 10:51:46
3	10.52.9.110:52002	192.168.1.0:60017	2008-02-04 10:50:15	2008-02-04 10:51:46
4	192.49.210:52003	192.168.1.0:60018	2008-02-04 10:40:16	2008-02-04 10:51:46

Client

The IP address and port on the NAT (or the client if there is no NAT) from which the STUN Relay request has come.

Relay Address

The IP address and port on the VCS that has been allocated for this particular relay request.

Expiry Time

The date and time at which the STUN Relay will become inactive.

Creation Time

The date and time on which the STUN Relay became active.

Applications

Viewing the Applications Page

The Applications page shows the status of all external applications running on the VCS. Currently this includes:

- Presence
- FindMe

To view the Applications page:

- Status > Applications

Understanding the Applications Page



Applications

All Applications that are installed on the VCS are shown on the left. Their current status is shown on the right.

Viewing the Warnings Page

The Warnings page provides a list of all the warnings currently in place on your system.

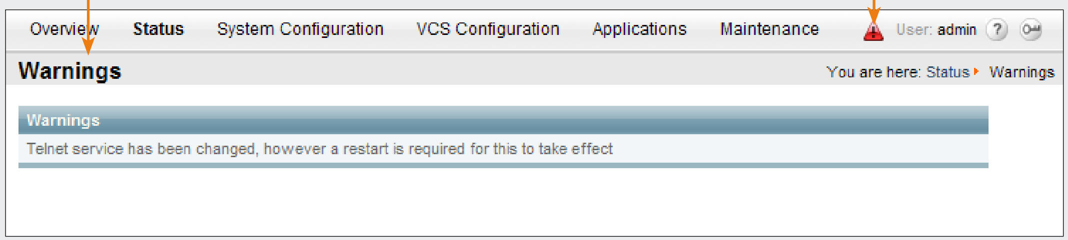
Warnings occur when an event or configuration change has taken place on the VCS that requires some manual Administrator intervention, such as a reboot.

When there are warnings in place on the VCS, a warning icon  will appear at the top right of the page.

To view the Warnings page, either:

- click on the  icon
- Status > Warnings

Understanding the Warnings Page



Warnings

Each warning (and, where relevant, its proposed resolution), is listed here.



System Warning

This icon appears on the top right corner of every page when there is a system warning in place. Click on this icon to go to the Warnings page which gives information about the warning and its suggested resolution.

Event Log

Viewing the Event Log Page

The Event Log page allows you to view and search the event log, which is a list of all the events that have occurred on your system since the last upgrade. The event log visible on the web UI holds a maximum 40 MB of data; once this size is reached, the oldest entries will be overwritten.

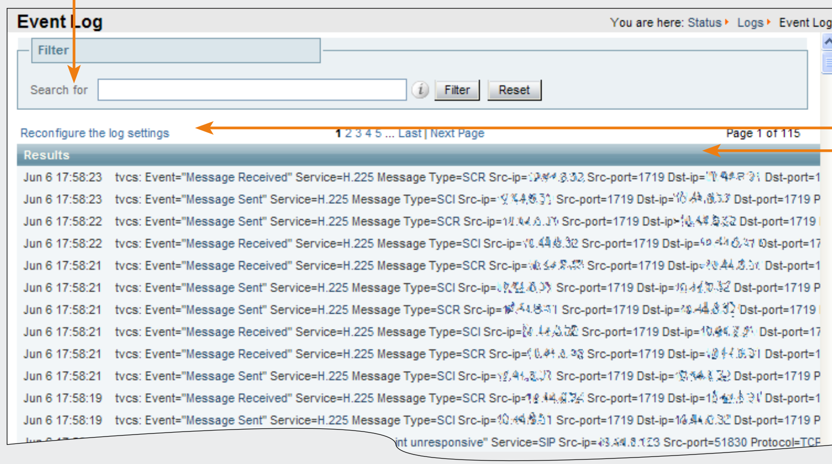
To view the Event Log page:

- Status > Logs > Event Log

You can also view the Event Log via the CLI:

- `eventlog`

Understanding the Event Log Page



Search for

This field allows you to filter the event log. Enter the text you wish to search for and click Filter. Only those events that contain the text you entered will then be shown.

To return to the complete Event Log listing, click Reset.

Reconfigure the log settings

Clicking this link will take you to the Logging configuration page. From this page, you can determine the level of events that are recorded in the Event Log, and also set up a remote server to which the Event Log can be copied.

Results

This section shows all the events, with the most recent being shown first.

Most `tvcs` events contain hyperlinks in one or more of the fields (such fields will change color when you hover over them). You can click on the hyperlink to show only those events that contain the same text string.

For example, clicking on the text that appears after `Event=` will filter the list to show all the events of that particular type. Likewise, clicking on a particular `Call-Id` will show just those events that contain a reference to that particular call.

Event Log Color Coding

Certain events in the Event Log are color-coded so that you can identify them more easily. These events are as follows:

Green

- System Start
- Installation of <item> succeeded
- Registration Accepted
- Call Connected
- Request Successful
- Beginning System Restore
- Completed System Backup
- Completed System Restore

Orange

- System Shutdown

Red

- Registration Rejected
- Registration Refresh Rejected
- Call Rejected
- License Limit Reached
- Decode Error
- TLS Negotiation Error
- External Server Communications Failure
- Application Failed
- Request Failed
- System Backup error
- System Restore error

Event Log Levels

You can configure the amount of detail that appears in the Event Log. See Setting the Event Log Level for more information.

Interpreting the Event Log

Event Log Format

The event log is displayed in an extension of the UNIX syslog format:

`date time process_name: message_details`

where:

Field	Description
`date`	the local date on which the message was logged
`time`	the local time at which the message was logged
`process_name`	the name of the program generating the log message. This could include: `tvcs` for all messages originating from TANDBERG VCS processes `web[ ]` for all web login and configuration events. but will differ for messages from third party processes which are used in the VCS product
`message_details`	the body of the message (see Message details field for further information)

Interpreting the Event Log

Message Details Field

For all messages logged from the tvcs process, the message _ details field, which contains the body of the message, consists of a number of human-readable name=value pairs, separated by a space.

The first field within the message _ details field is always Event and the last field is always Level.

The table below shows all the possible fields within the message _ details field, in the order that they would normally appear, along with a description of each.

In addition to the events described below, a syslog.info event containing the string MARK will be logged after each hour of inactivity to provide confirmation that logging is still active.

Field	Description
Event	The event which caused the log message to be generated. See Events and Levels for a list of all events that are logged by the VCS, and the level at which they are logged.
User	The username that was entered when a login attempt was made.
ipaddr	The source IP address of the user who has logged in.
Protocol	Specifies which protocol was used for the communication. Valid values are: • TCP • UDP • TLS.
Reason	Textual string containing any reason information associated with the event.
Service	Specifies which protocol was used for the communication. Will be one of: • H323 • SIP • H.225 • H.245 • LDAP • Q.931 • NeighbourGatekeeper • Clustering • ConferenceFactory.
Message Type	Specifies the type of the message.
ResponseCode	SIP response code or, for H.323 and interworked calls, a SIP equivalent response code.
Src-ip	Specifies the source IP address (the IP address of the device attempting to establish communications). This can be an IPv4 address or an IPv6 address.
Dst-ip	Specifies the destination IP address (the IP address of the destination for a communication attempt). The destination IP is recorded in the same format as Src-ip.
Dst-port	Specifies the destination port: the IP port of the destination for a communication attempt.

Field	Description
Src-port	Specifies the source port: the IP port of the device attempting to establish communications.
Src-Alias	If present, the first H.323 Alias associated with the originator of the message. If present, the first E.164 Alias associated with the originator of the message.
Dst-Alias	If present, the first H.323 Alias associated with the recipient of the message. If present, the first E.164 Alias associated with the recipient of the message.
Detail	Descriptive detail of the Event.
Auth	Whether the call attempt has been authenticated successfully.
Method	SIP method (INVITE, BYE, UPDATE, REGISTER, SUBSCRIBE, etc).
Contact	Contact: header from REGISTER.
AOR	Address of record.
Call-Id	The Call-ID header field uniquely identifies a particular invitation or all registrations of a particular client.
Call-Serial-Number	The VCS-local Call Serial Number that is common to all protocol messages for a particular call.
Tag	The Tag is common to all searches and protocol messages across a VCS network for all forks of a call.
To	(for REGISTER requests): the AOR for the REGISTER request.
RequestURI	The SIP or SIPS URI indicating the user or service to which this request is being addressed.
NumBytes	The number of bytes sent/received in the message.
Duration	Request/granted registration expiry duration.
Time	A full UTC timestamp in YYYY/MM/DD-HH:MM:SS format. Using this format permits simple ASCII text sorting/ordering to naturally sort by time. This is included due to the limitations of standard syslog timestamps.
Level	The level of the event as defined in Log Levels.

Events and Levels

Event	Description	Level
Admin Session Finish	An administrator has logged off the system.	1
Admin Session Login Failure	An unsuccessful attempt has been made to log in as an administrator. This could be because an incorrect username or password (or both) was entered.	1
Admin Session Start	An administrator has logged onto the system.	1
Application Failed	The VCS application is out of service due to an unexpected failure.	1
Application Start	The VCS has started. Further detail may be provided in the Detail event parameter.	1
Application Warning	The VCS application is still running but has experienced a recoverable problem. Further detail may be provided in the Detail event parameter.	1
Beginning System Backup	A system backup has started.	1
Beginning System Restore	A system restore has started.	1
Call Answer Attempted	An attempt to answer a call has been made.	1
Call Attempted	A call has been attempted.	1
Call Connected	A call has been connected.	1
Call Diverted	A call has been diverted.	1
Call Disconnected	A call has been disconnected.	1
Call Rejected	A call has been rejected. The Reason event parameter contains a textual representation of the H.225 additional cause code.	1
Completed System Backup	A system backup has completed.	1
Completed System restore	A system restore has completed.	1
Decode Error	A syntax error was encountered when decoding a SIP or H.323 message.	1
Eventlog Cleared	An operator cleared the event log.	1
External Server Communication Failure	Communication with an external server failed unexpectedly. The Detail event parameter should differentiate between 'no response' and 'request rejected'. Servers concerned are: • DNS • LDAP servers • Neighbor Gatekeeper • NTP servers • Peers	1
Hardware Failure	There is an issue with the VCS hardware. If the problem persists, contact your TANDBERG support representative.	1
License Limit Reached	Licensing limits for a given feature have been reached. The Detail event parameter specifies the facility/limits concerned. Possible values for the detail field are: • Non Traversal Call Limit Reached • Traversal Call Limit Reached	1

Event Log

Events and Levels

Event	Description	Level
Message Received	An incoming RAS message has been received.	2
Message Received	An incoming RAS NSM Keepalive, H.225 or H.245 message has been received.	3
Message Received	(SIP) An incoming message has been received.	4
Message Rejected	This could be for one of two reasons: 1. The VCS Authentication mode is set to On, and an endpoint has unsuccessfully attempted to send a message (such as a registration request) to the VCS. This could be either because the endpoint has not supplied any authentication credentials, or because its credentials do not match those expected by the VCS. 2. Clustering is enabled but bandwidth across the cluster has not been configured identically, and the VCS has received a message relating to an unknown Peer, Link, Pipe, Subzone or Zone. Use TMS to synchronize configuration across Peers.	1
Message Sent	An outgoing RAS message has been sent.	2
Message Sent	An outgoing RAS NSM Keepalive, H.225 or H.245 message has been sent.	3
Message Sent	(SIP) An outgoing message has been sent.	4
Policy Change	A policy file has been updated.	1
Registration Accepted	A registration request has been accepted.	1
Registration Refresh Accepted	A request to refresh or keep a registration alive has been accepted.	3
Registration Refresh Rejected	A request to refresh a registration has been rejected.	1
Registration Refresh Requested	A request to refresh or keep a registration alive has been received.	3
Registration Rejected	A registration request has been rejected. The Reason event parameter contains the H.225 cause code. Optionally, the Detail event parameter may contain a textual representation of the H.225 additional cause code.	1
Registration Removed	A registration has been removed by the VCS. The Reason event parameter specifies the reason why the registration was removed. This is one of: • Authentication change • Conflicting zones • Operator forced removal • Operator forced removal (all registrations removed) • Registration superseded.	1
Registration Requested	A registration has been requested.	1
Request Received	A call-related SIP request has been received.	2
Request Received	A non-call-related SIP request has been received.	3

Events and Levels

Event	Description	Level
Request Sent	A call-related SIP request has been sent.	2
Request Sent	A non-call-related SIP request has been sent.	3
Response Received	A call-related SIP response has been received.	2
Response Received	A non-call-related SIP response has been received.	3
Response Sent	A call-related SIP response has been sent.	2
Response Sent	A non-call-related SIP response has been sent.	3
System Backup error	An error has occurred while attempting a system backup.	1
System Configuration Changed	An item of configuration on the system has changed. The Detail event parameter contains the name of the changed configuration item and its new value.	1
System Restore error	An error has occurred while attempting a system restore.	1
System Shutdown	The operating system was shutdown.	1
System snapshot started	A system snapshot has been initiated.	1
System snapshot completed	A system snapshot has completed.	1
System Start	The operating system has started.	1
TLS Negotiation Error	Transport Layer Security (TLS) connection failed to negotiate.	1
Unregistration Accepted	An unregistration request has been accepted.	1
Unregistration Rejected	An unregistration request has been rejected.	1
Unregistration Requested	An unregistration request has been received.	1
User session finish	A FindMe user has logged out of the system.	1
User session Login failure	An unsuccessful attempt has been made to log in as a FindMe user. This could be because either an incorrect username or password (or both) was entered.	1
User session start	A FindMe user has logged on to the system.	1

Configuration Log

Viewing the Configuration Log Page

The Configuration Log page allows you to view and search login and configuration activities triggered via the VCS web interface. It shows all web login attempts for administrators and Findme users (both failed and successful), and all changes to the VCS configuration made via the web UI. The configuration log visible via the web UI holds a maximum of 4 MB of data; once this size is reached, the oldest entries will be overwritten.

To view the Configuration Log page:

- Status > Logs > Configuration Log

Search for

This field allows you to filter the configuration log. Enter the text you wish to search for and click Filter. Only those web-based events that contain the text you entered will then be shown.

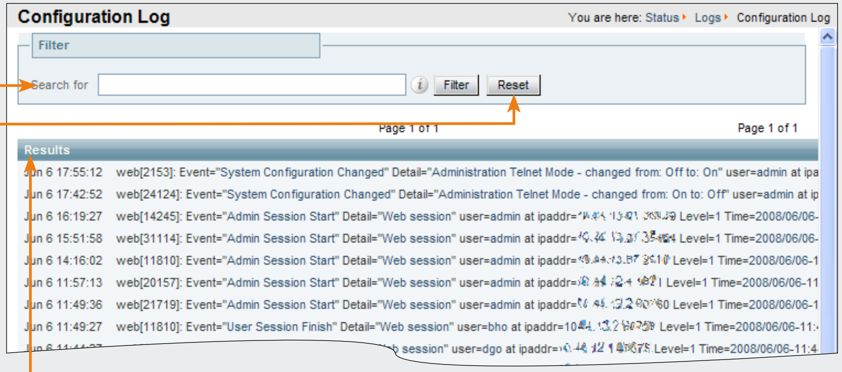
To return to the complete Configuration Log listing, click Reset.

Results

This section shows all the web-based events, with the most recent being shown first.

Most events contain hyperlinks in one or more of the fields (such fields will change color when you hover over them). You can click on the text that appears after `Event=` will filter the list to show all the events of that particular type. Likewise, clicking on a particular `user` will show just those events relating to that particular administration account.

Understanding the Configuration Log Page



All events that appear in the Configuration Log are also recorded in the Event Log. They are all recorded as Level 1 Events, so any changes to the Logging Levels will not affect their presence in the Configuration Log.

Types of Configuration Events

Administrator sessions

Will be one of the following Events:

- `Admin Session Start`
- `Admin Session Finish`
- `Admin Session Login Failure`

FindMe User sessions

Will be one of the following Events:

- `User Session Start`
- `User Session Finish`
- `User Session Login Failure`

For both of the above types of session, the Detail field for each of these events will include:

- the name of the administrator or FindMe user to whom the session relates, and their IP Address
- the date and time that the login was attempted, started, or ended.

Configuration changes

Changes to the VCS configuration made by administrators via the web UI will have an Event field of `System Configuration Changed`.

The Detail field of each of these events will give:

- the configuration item that was affected
- what it was changed from and to
- the name of the administrator user who made the change, and their IP Address
- the date and time that the change was made.

System Configuration

This section describes all the options that appear under the System Configuration menu of the web interface. These options enable you to configure the VCS in relation to the network in which it is located, for example its IP settings and the external services used by the VCS (e.g. DNS, NTP and SNMP).



System Administration

Overview

To configure the VCS's system administration settings:

- System Configuration > System.
  You will be taken to the System Administration page.
- xConfiguration SystemUnit Name
- xConfiguration Administration

About the System Name

The system name is used to identify the VCS. It appears in various places in the web interface, and in the display on the front panel of the unit (so that you can identify it when it is in a rack with other systems). The system name is also used by TANDBERG's TMS.

If no system name is specified, the LAN1 IPv4 address will be shown instead.

We recommend that you give the VCS a name that allows you to easily and uniquely identify it.

About Administrator Access settings

While it is possible to administer the TANDBERG VCS via a PC connected directly to the unit via a serial cable, you may wish to access the system remotely over IP.

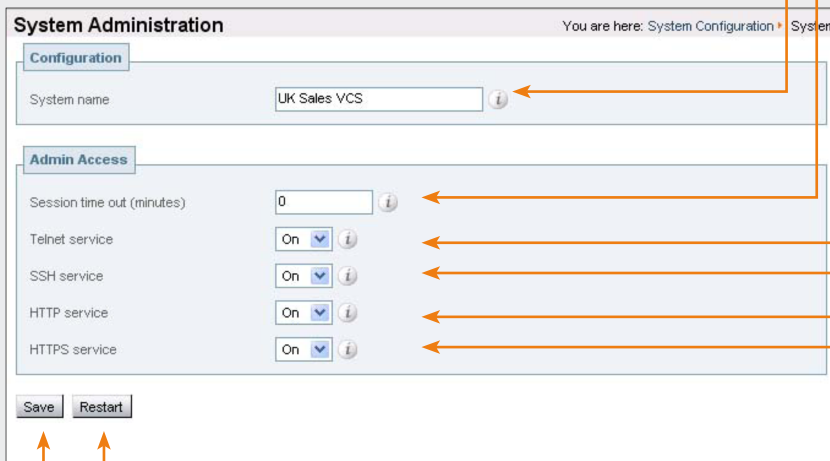
You can do this using either or both:

- the web interface via HTTPS
- a command line interface via SSH or Telnet.

By default, access via HTTPS and SSH is enabled; access via Telnet is disabled.

You can also enable access via HTTP. However, this mode works by redirecting HTTP calls to the HTTPS port, so HTTPS must also be enabled for access via HTTP to function.

Configuration



System name

Defines the name of the VCS. Choose a name that uniquely identifies the system.

Session time out (minutes)

Sets the number of minutes that an administration session (HTTPS, Telnet or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off.

Telnet service

Determines whether the VCS can be accessed via Telnet.

SSH service

Determines whether the VCS can be accessed via SSH and SCP.

HTTP service

On: HTTP calls will be redirected to the HTTPS port.

Off: no HTTP access will be available.

HTTPS service

Determines whether the VCS can be accessed via the web server. This must be On to enable both web interface and TMS access.

Save

Click here to save your changes.

Restart

Click here to restart the system.

You must save your changes and restart the system for any changes made via this page (apart from the Session time out) to take effect.

TMS accesses the VCS via the web server. If HTTPS mode is turned off, TMS will not be able to access it.

By default, access via HTTPS and SSH is enabled; access via Telnet is disabled. To securely manage the VCS you should disable Telnet, using the encrypted HTTPS and SSH protocols instead. For further security, disable HTTPS and SSH as well and use the serial port to manage the system.

Ethernet

Overview

To configure the VCS's Ethernet settings:

- System Configuration >Ethernet.
  You will be taken to the Ethernet page.
- xConfiguration Ethernet

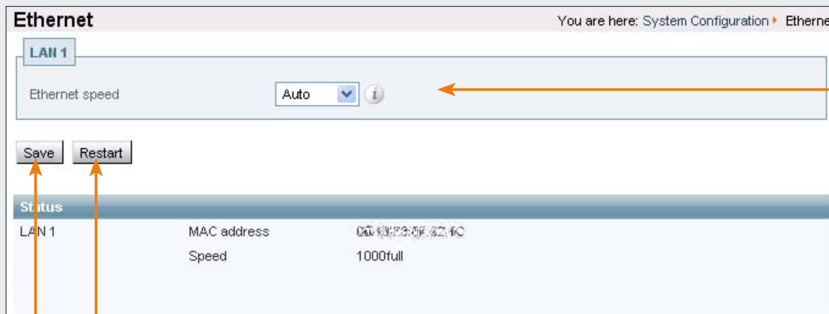
About Ethernet Speed

The Ethernet speed setting determines the speed of the connection between the VCS and the ethernet switch. It must be set to the same value on both systems.

The default is Auto, which means that the two systems will auto-negotiate the appropriate speed.

We recommend that you do not change from the default value of Auto unless the switch to which you are connecting is unable to auto-negotiate. A mismatch in Ethernet speed settings between the VCS and ethernet switch will at best result in packet loss; at worst it will make the system inaccessible for endpoints and system administrators.

Configuration



Ethernet speed

Sets the speed of the connection between the VCS and the ethernet switch.

If you have the Dual Network Interfaces option key installed, you will be able to configure this for both LAN1 and LAN2.

You must save your changes and restart the system for changes made via this page to take effect.

Restart

Click here to restart the system.

Save

Click here to save your changes.

Overview

To configure the VCS's IP settings:

- System Configuration > IP.
  You will be taken to the IP page.
- xConfiguration IP
- xConfiguration IPProtocol

About IPv4 to IPv6 Gatewaying

The VCS can act as a gateway between IPv4 and IPv6 calls. To enable this feature, select an IP Protocol of Both.

Some endpoints support both IPv4 and IPv6, however an endpoint can use only one protocol when registering with the VCS. Which protocol it uses will be determined by the format used to specify the IP address of the VCS on the endpoint. Once the endpoint has registered using one protocol, calls to it from an endpoint using the other protocol will be gatewayed by the VCS.

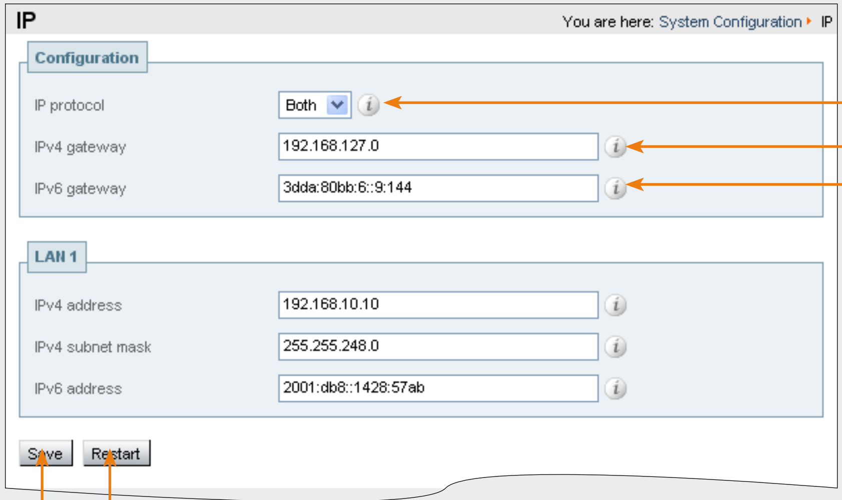
About IP Routes

The options on this page allow you to set the default IPv4 and IPv6 gateways used by the VCS. This is the gateway to which IP requests are sent for IP addresses that do not fall within the VCS's local subnet. However, you can also configure additional IP routing information on the VCS. This is sometimes required when using the Dual Network Interfaces option and occasionally required in other complex network deployments. You can configure routes for up to 50 networks and host combinations.

IP routes are configured via the CLI only using:

- xConfiguration IP Route
- xCommand RouteAdd

IP Configuration



Calls for which the VCS is acting as an IPv4 to IPv6 gateway are traversal calls. They will therefore require a traversal call licence.

IP protocol

You can configure the VCS to use IPv4, IPv6 or Both protocols. The default is Both.

IPv4: The VCS will only accept registrations from endpoints using an IPv4 address, and will only take calls between two endpoints communicating via IPv4. It will communicate with other systems via IPv4 only.

IPv6: The VCS will only accept registrations from endpoints using an IPv6 address, and will only take calls between two endpoints communicating via IPv6. It will communicate with other systems via IPv6 only.

Both: The VCS will accept registrations from endpoints using either an IPv4 or IPv6 address, and will take calls using either protocol. If a call is between an IPv4-only and an IPv6-only endpoint, the VCS will act as an IPv4 to IPv6 gateway. It can communicate with other systems via either protocol.

IPv4 gateway

Specifies the default IPv4 gateway of the VCS.

IPv6 gateway

Specifies the default IPv6 gateway of the VCS.

Restart

Click here to restart the system.

Save

Click here to save your changes.

You must save your changes and restart the system for changes to take effect.

Overview

To configure the VCS's LAN 1 and LAN 2 ethernet port settings:

- System Configuration > IP.
  You will be taken to the IP page.
- xConfiguration Ethernet

The VCS is shipped with a default IP address for LAN 1 of 192.168.0.100. This allows you to connect the VCS to your network and access it via the default address so that you can configure it remotely.

About LAN Configuration

LAN 1 is the primary network port on the VCS. You can configure the IPv4 address and subnet mask, and IPv6 address for this port.

In addition, if you have the Dual Network Interface option key installed, you will also be able to configure the LAN 2 port.

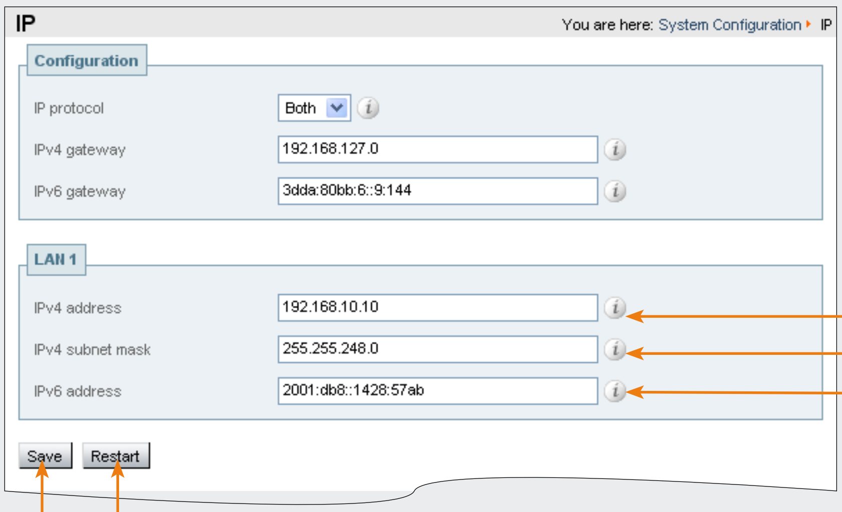
About Dual Network Interfaces

The Dual Network Interface option enables the LAN 2 port on the VCS for both management and call signaling. This allows you to have a secondary IP address for your VCS.

This configuration is intended for high-security deployments where the VCS is located in a DMZ between two separate firewalls on separate network segments. In such deployments, routers prevent devices on the internal network from being able to route IP traffic to the public internet, and instead the traffic must pass through an application proxy such as the VCS.

To enable this feature you must purchase and install the appropriate Option Key. Contact your TANDBERG representative for information.

LAN Configuration



IPv4 address
Specifies the IPv4 IP address of the VCS's LAN1 port.

IPv4 subnet mask
Specifies the IPv4 subnet mask of the VCS's LAN1 port.

IPv6 address
Specifies the IPv6 address of the VCS's LAN1 port.

If you have the Dual Network Interfaces option key installed, you will also be able to configure the IPv4 address, IPv4 subnet mask and IPv6 address for the LAN2 port via this page.

Restart
Click here to restart the system.

Save
Click here to save your changes.

You must save your changes and restart the system for changes to take effect.

Overview

About DNS Servers

You must specify at least one DNS server to be queried for address resolution if you wish to either:

- use FQDNs (Fully Qualified Domain Names) instead of IP addresses when specifying external addresses (for example for LDAP and NTP servers, neighbor zones and alternates), or
- use features such as URI dialing or ENUM dialing.

You can specify up to 5 DNS servers. The VCS sends requests to all configured servers in parallel taking the first result received and discounting the rest.

This can lead to confusing behavior should local network administrators, for example, deploy 'split horizon' DNS where records held on an internal, corporate, DNS server use the same domain names but with different values to those on the public internet - an often used tactic in corporate intranets.

About the DNS Domain Name

The DNS Domain Name is used when attempting to resolve server addresses configured on the VCS that are without any form of qualification (e.g. ldap or ldap_server but not ldap.server). It applies only to the following:

- LDAP server
- NTP server
- External Manager server
- Remote logging server.

The DNS Domain Name is appended to the unqualified server address before a query to the DNS server is executed.

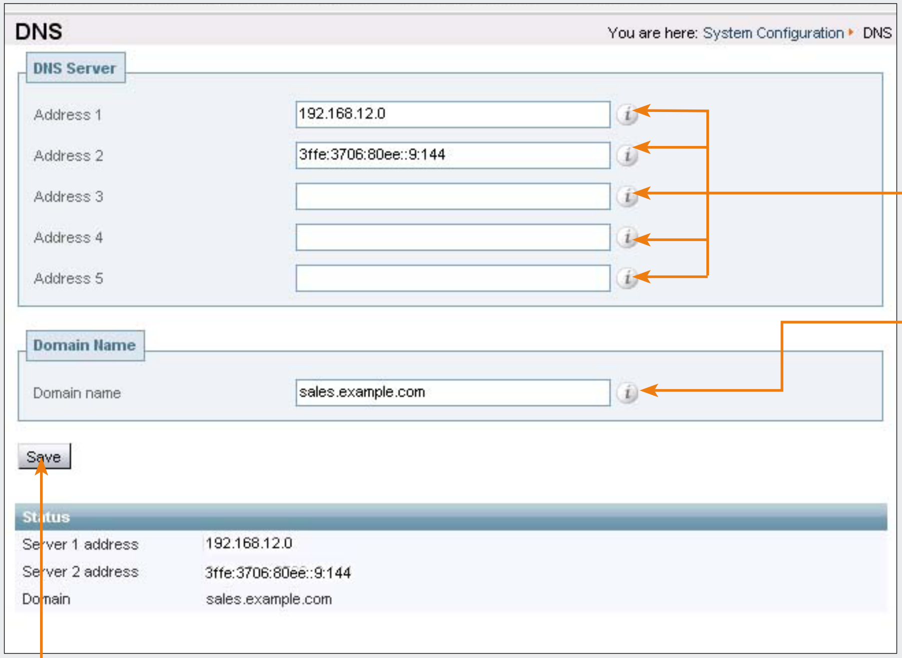
If the server address is an IP address or is in the format of a domain name, DNS will only be queried for the server address as configured, without the DNS Domain Name appended. For this reason we recommend that all server addresses use an IP address or FQDN (Fully Qualified Domain Name).

The DNS Domain name plays no part in URI dialing.

Configuration

To configure the VCS's DNS settings:

- System Configuration > DNS.
  You will be taken to the DNS page.
- xConfiguration IP DNS



Address 1 to Address 5
Sets the IP address of a DNS server to be queried when resolving domain names.

Domain name
Specifies the name to be appended to an unqualified server address before a query to the DNS server is executed.

Save
Click here to save your changes.

NTP

Overview

To configure the VCS's NTP settings:

- System Configuration > NTP
  You will be taken to the NTP page.
- xConfiguration NTP Address
- xConfiguration TimeZone Name

About the NTP Server

The NTP server is a remote server with which the VCS synchronizes in order to ensure its time setting is accurate. The NTP server provides the VCS with UTC time.

Accurate timestamps play an important part in authentication, helping to guard against replay attacks. For this reason, if you are using authentication, both the VCS and the endpoints must use an NTP server to synchronize their system time.

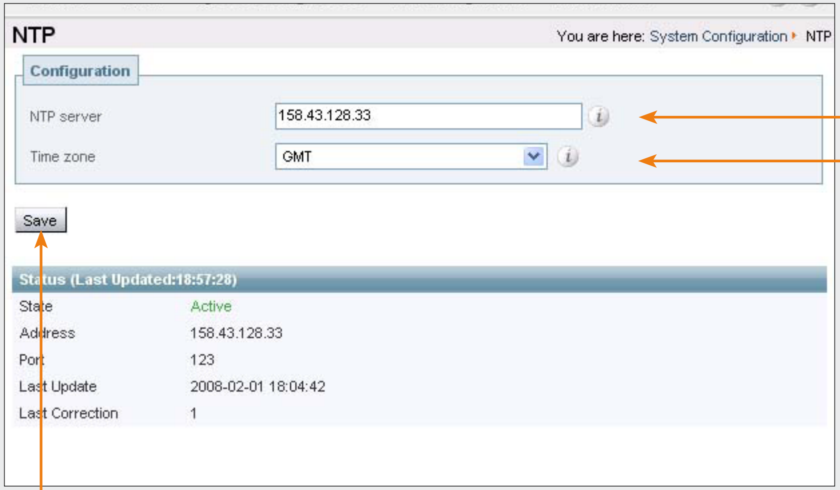
Traversal clients must always authenticate with traversal servers, even if the server's Authentication Mode is Off. Therefore in order for a traversal client and traversal server to connect to each other, both must be configured with details of an NTP server.

About the Time Zone

The NTP server provides the VCS with UTC time. You can also determine the local time to be used on your system by configuring the Time Zone. This takes the UTC time and offsets it by the number of hours specified by the selected time zone to make the local time.

The local time is used throughout the web UI and to set the timestamp that appears at the start of each line in the Event Log.

Configuration



NTP server

Sets the IP address or FQDN (or server address, if a DNS Domain Name has also been configured) of the NTP server to be used when synchronizing system time.

Time zone

Sets the local time zone of the VCS.

Save

Click here to save your changes.

SNMP

Overview

About SNMP

Tools such as TANDBERG Management Suite (TMS) or HP OpenView may act as SNMP Network Management Systems (NMS). They allow you to monitor your network devices, including the VCS, for conditions that might require administrative attention.

The VCS supports the most basic MIB-II tree (.1.3.6.1.2.1) as defined in RFC 1213 [23]. The information made available by the VCS includes the following:

- system uptime
- system name
- location
- contact
- interfaces
- disk space, memory, and other machine-specific statistics.

To allow the VCS to be monitored by an SNMP NMS (including TMS), you must Enable SNMP on the VCS and provide the name of the SNMP community within which it resides. You may optionally provide the name of a System contact and the physical Location of the system for reference by administrators when following up on queries.

By default, SNMP is Disabled with a SNMP community name of public.

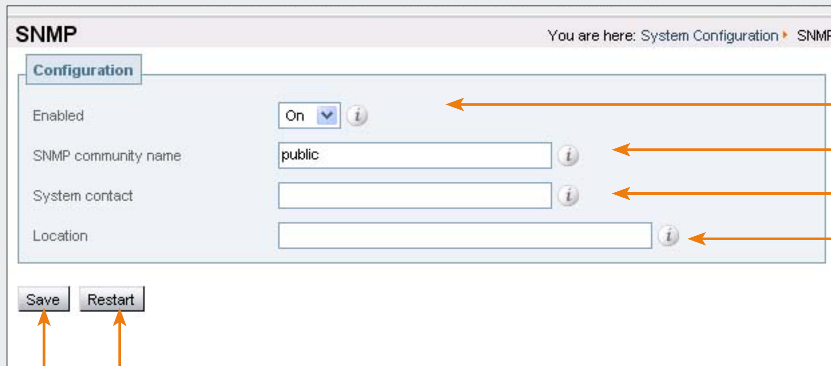
The VCS does not support SNMP traps or SNMP sets, therefore it cannot be managed via SNMP.

SNMP is disabled by default, because of the potentially sensitive nature of the information involved. Do not enable SNMP on a VCS on the public internet or in any other environment where you do not want to expose internal system information.

Configuration

To configure the VCS's SNMP settings:

- System Configuration > SNMP
  You will be taken to the SNMP page.
- xConfiguration SNMP



Enabled
Select On to enable SNMP support.

You must save your changes and restart the system for any changes to take effect.

SNMP community name
Sets the VCS's SNMP community name.

System contact
Specifies the name of the person who can be contacted regarding issues with the VCS.

Location
Specifies the physical location of the VCS.

Restart
Click here to restart the system.

Save
Click here to save your changes.

External Manager

Overview

To configure the VCS's External Manager settings:

- System Configuration > External Manager. You will be taken to the External Manager page.
- `xConfiguration ExternalManager`

About the External Manager

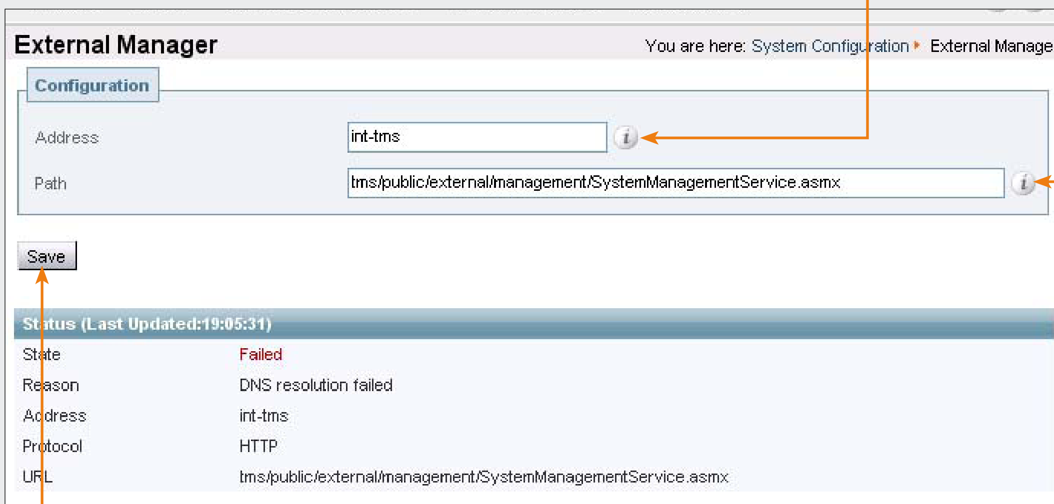
An External Manager is a remote system, such as the TANDBERG Management Suite (TMS), used to monitor events occurring on the VCS, for example call attempts, connections and disconnections.

The use of an External Manager is optional.

In order to use an External Manager, you must configure the VCS with the IP address or host name and path of the External Manager to be used.

If you are using TMS as your external manager, use the default path of `tms/public/external/management/SystemManagementService.asmx`.

Configuration



Address

Sets the IP address or FQDN (or server address, if a DNS Domain Name has also been configured) of the External Manager.

Path

Sets the path of the External Manager.

Save

Click here to save your changes.

Logging

Overview

About Logging

The VCS provides an event logging facility for troubleshooting and auditing purposes. The event log records information about such things as calls, registrations, and messages sent and received.

The VCS logging facility allows you to:

- specify the amount of information that is logged. This is done by changing the event log level
- copy the event log to a remote syslog server.

Remote Logging

About Remote Logging

The event log is always stored locally on the VCS. However, it is often convenient to collect copies of all event logs from various systems in a single location. A computer running a BSD-style syslog server, as defined in RFC 3164 [4], may be used as the central log server.

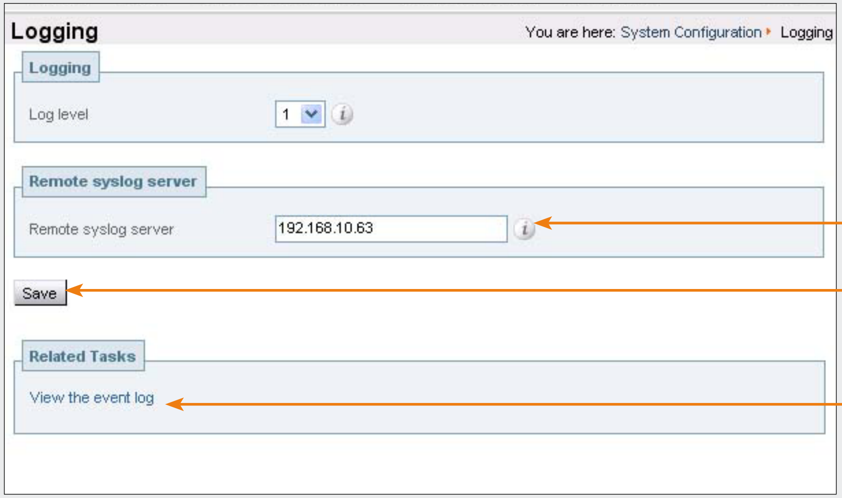
A VCS will not act as a central logging server for other systems.

Enabling Remote Logging

To enable remote logging, you must configure the VCS with the address of the central log server to which the event log will be copied. To do this:

- System Configuration > Logging.
  You will be taken to the Logging page.
- xConfiguration Log Server Address

Events will be always logged locally (i.e. to the Event Log) regardless of whether or not remote logging has been enabled.



Remote syslog server

Enter the IP address or FQDN (or server address, if a DNS Domain Name has also been configured) of the server to which the log will be written.

This server must support the BSD syslog protocol. It cannot be another VCS.

Save

Click here to save your changes.

View the Event Log

Clicking on this link will take you to the Event Log page, which displays the Event Log.

Log Levels

About Event Log Levels

All events have an associated level in the range 1-4, with level 1 events considered the most important. The table below gives an overview of the levels assigned to different events.

See Events and Levels for a list of all events that are logged by the VCS, and the level at which they are logged.

Level	Assigned Events
Level 1	High-level events such as registration requests and call attempts. Easily human readable. For example: • call attempt/connected/disconnected • registration attempt/accepted/rejected.
Level 2	All Level 1 Events, plus: • Logs of protocol messages sent and received (H.323, LDAP, etc.) excluding noisy messages such as H.460.18 keepalives and H.245 video fast-updates.
Level 3	All Level 1 and Level 2 Events, plus: • Protocol keepalives
Level 4	All Level 1, Level 2 and Level 3 Events, plus: • SIP messages

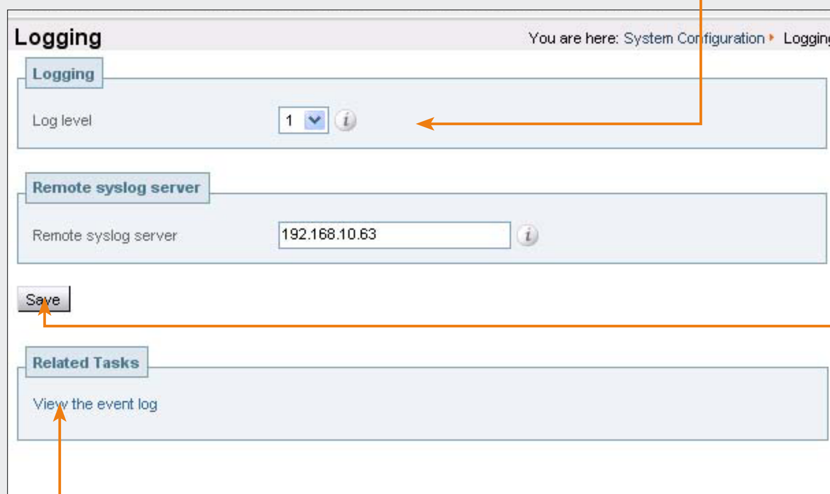
We do not usually recommend logging at Level 3 or Level 4, as the Event Log holds a maximum of 40 MB of data and logging at these levels on a busy system could cause the Event Log to be recycled too quickly.

Setting the Event Log Level

You can control which events are logged by the VCS by setting the log level. All events with a level numerically equal to and lower than the specified logging level are recorded in the event log. So, at Level 1, only Level 1 events are logged; at Level 2, both Level 1 and Level 2 events are logged, etc.

To set the log level:

- System Configuration > Logging.
  You will be taken to the Logging page.
- `xConfiguration Log Level`



Log level

Select the level of logging you require.

The default is 1.

Changes to the event log level affect both the event log that you can view via the web interface, and the information that is copied to the remote log server (if any) that you have configured.

Changes to the event log level are not retrospective. If you change the event log level, it will only effect what is logged from that point onwards.

Save

Click here to save your changes.

View the Event Log

Clicking on this link will take you to the Event Log page, where you can view and search the Event Log.

VCS Configuration

This section provides information on the pages that appear under the Protocols, Registrations and Authentication sub-menus of the VCS Configuration menu. These pages allow you to configure the functionality of the VCS in each of these areas.

This section includes the following information:

- an overview of H.323 and the H.323 configuration options available on the VCS
- an overview of SIP and the SIP configuration options available on the VCS
- how to configure the VCS to act as a SIP to H.323 gateway
- how to control registrations on the VCS using authentication and Allow Lists and Deny Lists.



H.323 Overview

About H.323 on the VCS

The VCS supports the H.323 protocol: it is an H.323 gatekeeper. It will also provide interworking between H.323 and SIP, translating between the two protocols to enable endpoints that only support one of these protocols to call each other. In order to support H.323, the H.323 mode must be enabled.

Using the VCS as an H.323 Gatekeeper

As an H.323 gatekeeper, the VCS accepts registrations from H.323 endpoints and provides call control functions such as address translation and admission control.

Configuring H.323 Ports

The VCS allows you to configure the listening port for H.323 registrations and call signaling, and the range of ports to be used by H.323 calls once they are established.

The default VCS configuration uses standard port numbers so you can use H.323 services out of the box without having to first set these up.

H.323 Endpoint Registration

Overview

H.323 endpoints in your network must register with the VCS in order to use it as their gatekeeper.

There are two ways an H.323 endpoint can locate a VCS with which to register: manually or automatically. The option is configured on the endpoint itself under the Gatekeeper Discovery setting (consult your endpoint manual for how to access this setting).

- If the mode is set to automatic, the endpoint will try to register with any VCS it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible VCSs will respond.
- If the mode is set to manual, you must specify the IP address of the VCS with which you wish your endpoint to register, and the endpoint will attempt to register with that VCS only.

Registration Conflict Mode

An H.323 endpoint may attempt to register with the VCS using an alias that has already been registered on the VCS from another IP address. The reasons for this could include:

- two endpoints at different IP addresses are attempting to register using the same alias
- a single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint then changes, and the endpoint is attempting to re-register using the same alias.

You can determine how the VCS will behave in this situation by configuring the Registration Conflict Mode. The options are:

- Reject: denies the new registration.
- Overwrite: deletes the original registration and replaces it with the new registration.

Auto Discover

The VCS has an Auto Discover setting which determines whether it will respond to the Gatekeeper Discovery Requests sent out by endpoints.

To prevent H.323 endpoints being able to register automatically with the VCS, set Auto Discover to Off. This will mean that endpoints will be able to register with the VCS only if they have been configured with the VCS's IP address.

Time to Live

H.323 endpoints must periodically re-register with the VCS in order to confirm that they are still functioning. The VCS allows you to configure the interval (in seconds) between these re-registrations, known as the Time to Live.

Some older endpoints do not support the ability to periodically re-register with the system. In this case, and in any other situation where the system has not had a confirmation from the endpoint within the specified period, it will send an IRQ to the endpoint to verify that it is still functioning.

Call Time to Live

Once the endpoint is in a call, the VCS will periodically poll it to confirm whether it is still in the call. If the endpoint does not respond, the call will be disconnected.

The VCS allows you to configure the interval (in seconds) at which the endpoints are polled, known as the Call Time to Live.

The system will poll endpoints in a call regardless of whether the call type is traversal or non-traversal.

Configuring H.323

To configure the VCS's H.323 settings:

- VCS Configuration > Protocols > H.323.
  You will be taken to the H.323 page.
- xConfiguration H323

H.323 Mode

Determines whether or not the VCS will provide H.323 gatekeeper functionality.

Registration UDP port

Specifies the port to be used for H.323 UDP registrations.

The default is 1719.

Call signaling TCP port

Specifies the port that listens for H.323 call signaling.

The default is 1720.

Call signaling port range start

Specifies the lower port in the range to be used by H.323 calls once they are established.

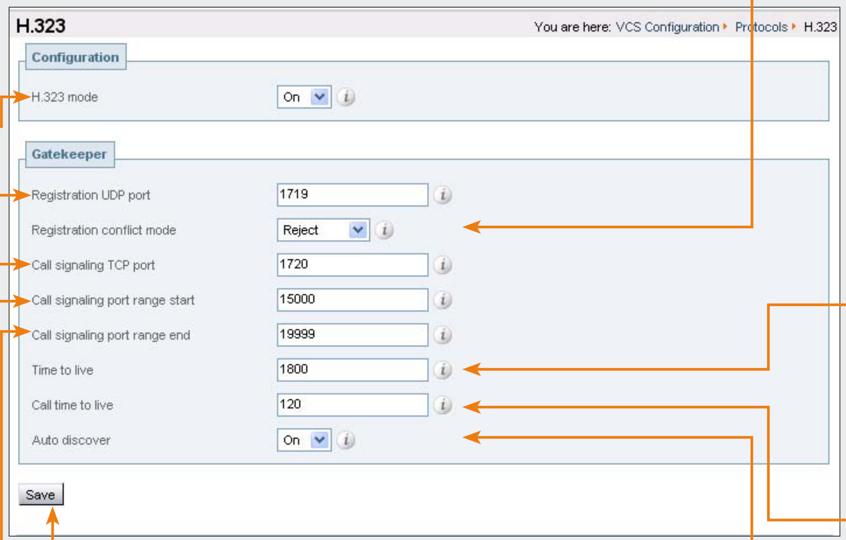
The default is 15000.

Call signaling port range end

Specifies the upper port in the range to be used by H.323 calls once they are established.

The default is 19999.

The call signalling port range must be great enough to support all the required concurrent calls.



Registration conflict mode

Determines how the system will behave if an endpoint attempts to register an alias currently registered from another IP address.

Reject: denies the registration.

Overwrite: deletes the original registration and replaces it with the new registration.

The default is Reject.

Time to live

Specifies the interval (in seconds) at which an H.323 endpoint must re-register with the VCS in order to confirm that it is still functioning.

The default is 1800.

Call time to live

Specifies the interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call

The default is 120.

Auto discover

Determines whether or not the VCS responds to gatekeeper discovery requests from endpoints.

The default is On.

Save

Click here to save your changes.

SIP Overview

About SIP on the VCS

The VCS supports the SIP protocol. It can act as a:

- SIP Registrar
- SIP Proxy
- SIP Presence Server.

The VCS will provide interworking between SIP and H.323 calls. In order to support SIP, SIP mode must be enabled and at least one of the SIP transport protocols (i.e. UDP, TCP or TLS) must be active.

Using the VCS as a SIP Registrar

In order for a SIP endpoint to be contactable via its registered alias, it must register its location with a SIP Registrar. The VCS can act as a SIP Registrar for up to 20 domains.

SIP aliases always take the form username@domain. To enable the VCS to act as a SIP Registrar, you must configure it with the SIP Domain(s) for which it will be authoritative. It will then accept registration requests for any endpoints attempting to register with an alias that includes that domain.

If no Domains are configured, then the VCS will not act as a SIP Registrar.

Proxying Registration Requests

If the VCS has no domains configured, or it receives a registration request for a domain for which it is not acting as a Registrar, then the VCS may proxy the registration request. This depends on the SIP Registration Proxy Mode setting, as follows:

- Off: the VCS will not proxy any registration requests. The request will be rejected with a "`403 Forbidden`" message.
- Proxy to Known Only: the VCS will proxy the registration request but only to its Neighbor, Traversal Client and Traversal Server zones.
- Proxy to any: the VCS will proxy the registration requests in accordance with its call policy (e.g. Administrator policy and transforms). See Call Processing for more information.

The SIP Registration Proxy Mode setting also impacts the VCS's behavior when acting as a SIP Proxy Server.

SIP Registration Expiry

SIP endpoints must periodically re-register with the SIP Registrar in order to prevent their registration expiring. You can configure the interval with which SIP endpoints must register with the VCS.

The SIP Registration Expiry setting applies only when the VCS is acting as a SIP Registrar, and to endpoints registered with the VCS. It does not apply to endpoints whose registrations are being proxied through the VCS.

SIP Overview

Using the VCS as a SIP Proxy Server

When SIP mode has been enabled the VCS may act as a SIP Proxy Server. The role of a Proxy Server is to forward requests (such as REGISTER and INVITE) from endpoints or other Proxy Servers. These requests are forwarded on to other Proxy Servers or to the destination endpoint.

Whether or not the VCS acts as a SIP Proxy Server, and its exact behavior when proxying requests, is determined by the SIP Registration Proxy Mode setting. In addition, this also depends on the presence of Route Set information in the request header and whether or not the Proxy Server from which the request was received is a Neighbor of the VCS.

A Route Set can specify the path that must be taken when requests are being proxied between an endpoint and its Registrar. For example, when a REGISTER request is proxied by a VCS, the VCS adds a Path header component to the request which signals that the VCS must be included on any call to that endpoint. The information is usually required in situations where firewalls exist and the media must follow a specified path in order to successfully traverse the firewall. For more information about the path header field, see RFC 3327 [10].

When the VCS proxies a request that contains existing Route Set information, it will forward it directly to the URI specified in the path. Any call policy configured on the VCS will therefore be bypassed. This may present a security risk if the information in the Route Set cannot be trusted. For this reason, you can configure the VCS with three different behaviors when proxying requests, as follows:

- If the SIP Registration Proxy Mode setting is Off, the VCS will not proxy any requests that have an existing Route Set. Requests that do not have an existing Route Set will still be proxied in accordance with existing call policy (e.g. zone searches and transforms). This setting provides the highest level of security.
- If the setting is Proxy to Known Only, the VCS will proxy requests with an existing Route Set only if the request was received from a Neighbor zone (including Traversal Client and Traversal Server zones). Requests that do not have an existing Route Set will be proxied in accordance with existing call policy.
- If the setting is Proxy to any, the VCS will proxy all requests. Those with existing Route Sets will be proxied to the specified URI; those without will be proxied in accordance with existing call policy.

The SIP Registration Proxy Mode setting only applies to dialog-forming requests, e.g. INVITE and SUBSCRIBE. Responses, such as NOTIFY, are always proxied regardless of this setting.

Using the VCS as a SIP Presence Server

The VCS supports the SIP-based SIMPLE protocol. It can act as a:

- Presence Server
- Presence User Agent

for any of the SIP Domain(s) for which it is authoritative.

For full information on how to use the VCS as a SIP Presence server, see the Presence section.

SIP protocols and ports

The VCS supports SIP over UDP, TCP and TLS transport protocols. You can configure whether or not incoming calls using each protocol are supported, and if so, the ports on which the VCS will listen for such calls. You can also specify the range of ports the VCS will use once calls are established. This range must be sufficient to support all required concurrent calls.

At least one of the UDP, TCP or TLS transport protocols must be set to a Mode of On in order for SIP functionality to be supported.

Configuring SIP - Registrations, Protocols and Ports

SIP settings are configured via:

- VCS Configuration > Protocols > SIP > Configuration.
  You will be taken to the SIP page.
- xConfiguration SIP

SIP mode

Determines whether or not the VCS will provide SIP functionality (i.e. SIP Registrar and SIP proxy services).

Registration expire delta

Specifies the period (in seconds) within which a SIP endpoint must re-register to prevent its registration expiring.

The default is 60.

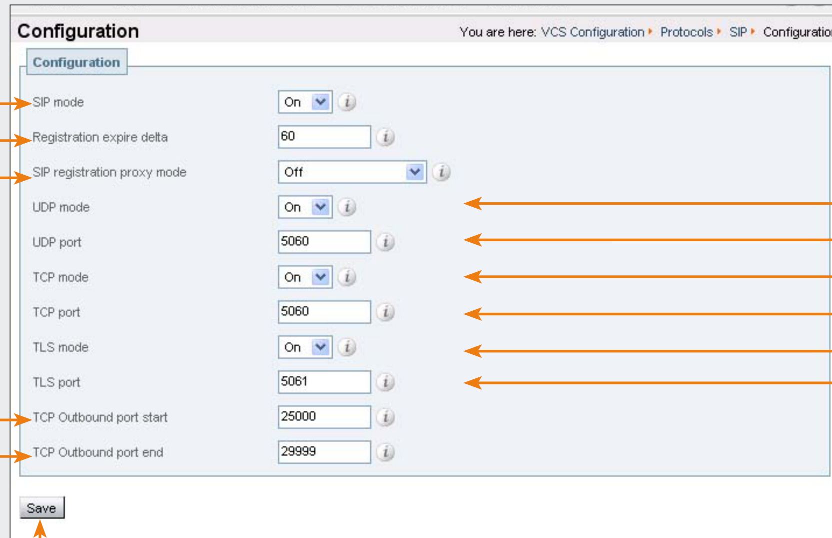
SIP registration proxy mode

Specifies how proxied registrations and invites will be handled.

Off: Registration requests will not be proxied (but will still be permitted locally if the VCS is authoritative for that domain). Invite requests with existing Route Sets will be rejected.

Proxy to known only: Registration requests will be proxied, and invite requests will be proxied only if the Route Set contains the URI(s) of neighbors (including traversal clients and traversal servers).

Proxy to any: Registration requests and invite requests will always be proxied.



UDP mode

Determines whether or not incoming SIP calls using the UDP protocol will be allowed.

The default is On.

UDP port

Specifies the listening port for incoming SIP calls over UDP.

The default is 5060.

TCP mode

Determines whether or not incoming SIP calls using the TCP protocol will be allowed.

The default is On.

TCP port

Specifies the listening port for incoming SIP calls over TCP.

The default is 5060.

TLS mode

Determines whether or not incoming SIP calls using the TLS protocol will be allowed.

The default is On.

TLS port

Specifies the listening port for incoming SIP calls over TLS.

The default is 5061.

TCP Outbound Port Start

Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections.

The default is 25000.

TCP Outbound Port End

Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections.

The default is 29999.

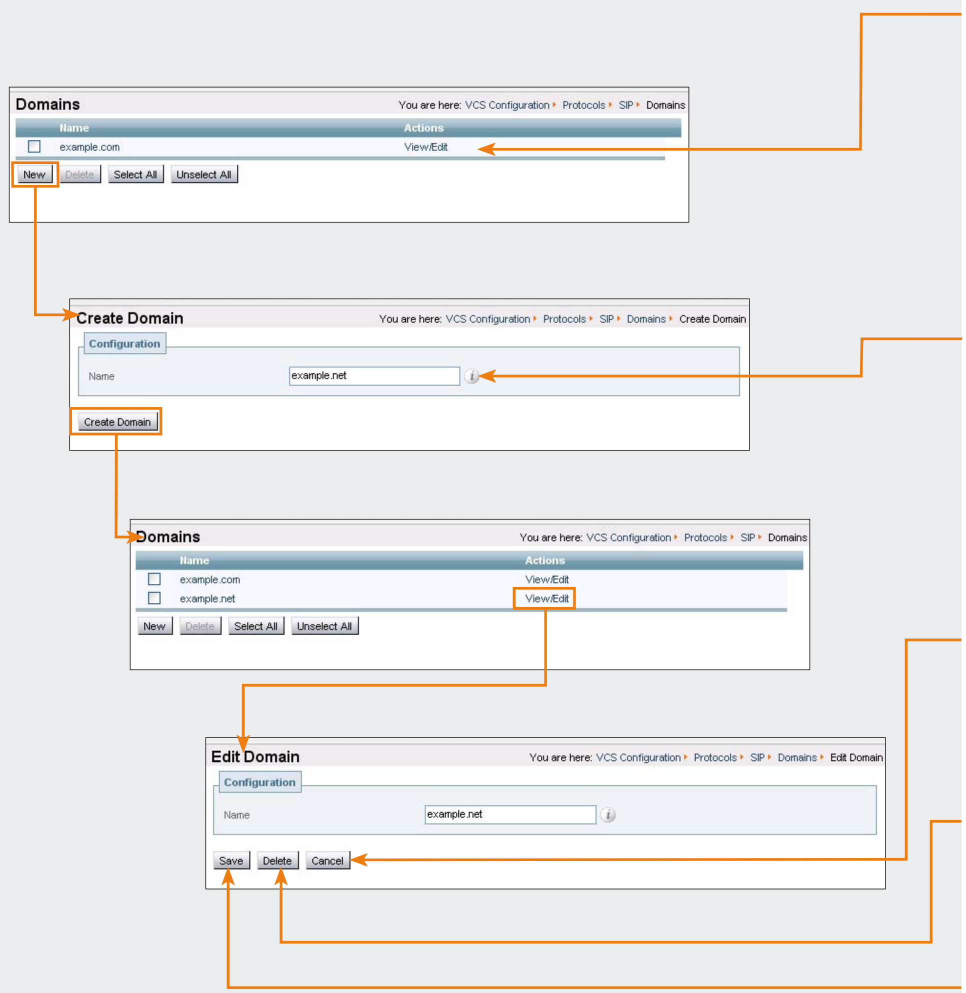
Save

Click here to save your changes.

Configuring SIP - Domains

SIP domains are configured via:

- VCS Configuration > Protocols >SIP > Domains.
  You will be taken to the Domains page.
- To add a new domain, click New.
  You will be taken to the Create Domain page.
  Enter the domain in the Name field and click Create Domain.
  The new domain will be added and you will be returned to the Domains page.
- To edit the name of an existing domain, click View/Edit.
  You will be taken to the Edit Domain page.
  Edit the Name of the domain and click Save.
  The name of the domain will be changed.
- To delete an existing domain, click View/Edit.
  You will be taken to the Edit Domain page.
  Click Delete.
  The domain will be deleted and you will be returned to the Domains page.
- To delete one or more existing domains, select the boxes next to the domains you wish to delete and click Delete.
- xCommand DomainAdd
- xCommand DomainDelete
- xConfiguration SIP Domains



View/Edit
Click here to change the domain name or delete the domain.

Name
Specifies a domain for which the VCS is authoritative.

The VCS will act as a SIP Registrar and Presence Server for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain.

Cancel
Click here to return to the Domains page without saving your changes.

Delete
Click here to delete the domain and return to the Domains page.

Save
Click here to save your changes.

Overview

About Interworking

The VCS is able to act as a gateway between SIP and H.323, translating calls from one protocol to the other. This is known as "interworking".

By default, the VCS will act as a SIP-H.323 and H.323-SIP gateway but only if at least one of the endpoints is locally registered.

You can change this setting so that the VCS will act as SIP-H.323 gateway regardless of whether the endpoints involved are locally registered.

You also have the option to disable interworking completely.

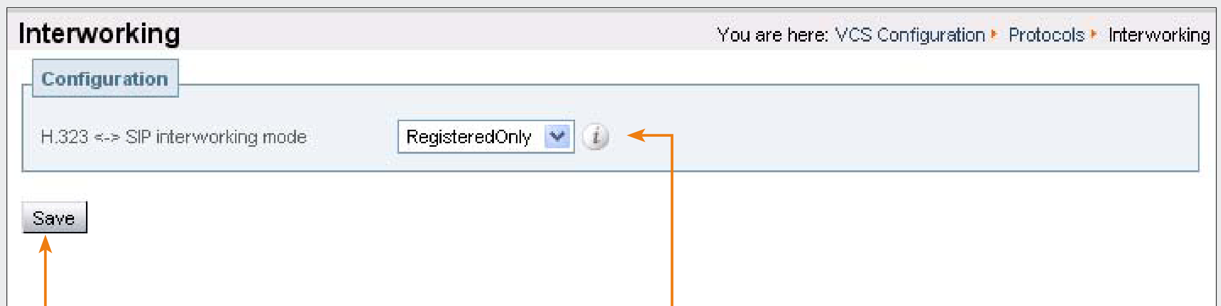
We recommend that you leave this setting as RegisteredOnly (where calls are interworked only if at least one of the endpoints is locally registered). Unless your network is correctly configured, setting it to On (where all calls can be interworked) may result in unnecessary interworking, for example where a call between two H.323 endpoints is made over SIP, or vice versa.

Calls for which the VCS is acting as an SIP to H.323 gateway are traversal calls. They will therefore require a traversal call licence.

Configuring Interworking

Interworking options are configured via:

- VCS Configuration > Protocols > Interworking. You will be taken to the Interworking page.
- `xConfiguration Interworking Mode`



Save

Click here to save your changes.

H.323 <-> SIP interworking mode

Determines whether or not the VCS will act as a gateway between SIP and H.323 calls.

Off: the VCS will not act as a SIP-H.323 gateway.

RegisteredOnly: the VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.

On: the VCS will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered.

Registration Control

Registration Overview

Endpoint Registration

In order for an endpoint to use the TANDBERG VCS as its H.323 gatekeeper or SIP Registrar, the endpoint must first register with the VCS. The VCS can be configured to control which devices are allowed to register with it. Two separate mechanisms are provided:

- an authentication process based on the username and password supplied by the endpoint
- a simple Registration Restriction Policy that uses Allow Lists or Deny Lists to specify which aliases can and cannot register with the VCS.

It is possible to use both mechanisms together. For example, you can use authentication to verify an endpoint's identity from a corporate directory, and registration restriction to control which of those authenticated endpoints may register with a particular VCS.

This section gives an overview of how endpoints and other devices register with the VCS, and then describes the two mechanisms by which registrations can be restricted.

For specific information about how registrations are managed across Peers in a cluster, refer to the section Sharing Registrations Across Peers.

Registrations on a VCS Expressway

If a traversal-enabled endpoint registers directly with a VCS Expressway, the VCS Expressway will provide the same services to that endpoint as a VCS Control, with the addition of firewall traversal. Traversal-enabled endpoints include all TANDBERG Expressway™ endpoints and third party endpoints which support the ITU H.460.18 and H.460.19 standards.

Endpoints that are not traversal-enabled can still register with a VCS Expressway, but they may not be able to make or receive calls through the firewall successfully. This will depend on a number of factors:

- whether the endpoint is using SIP or H.323
- the endpoint's position in relation to the firewall
- whether there is a NAT in use
- whether the endpoint is using a public IP address.

For example, if an endpoint is behind a NAT or firewall, it may not be able to receive incoming calls and may not be able to receive media for calls it has initiated. SIP endpoints can also work behind a NAT but can only receive video if they send it as well.

To ensure firewall traversal will work successfully for H.323 endpoints behind a NAT, the endpoint must be traversal-enabled.

MCU, Gateway and Content Server Registration

H.323 systems such as gateways, MCUs and Content Servers can also register with a VCS. They are known as locally registered services. These systems are configured with their own prefix, which they provide to the VCS when registering. The VCS will then know to route all calls that begin with that prefix to the gateway, MCU or Content Server as appropriate. These prefixes can also be used to control registrations.

SIP devices cannot register prefixes. If your dial plan dictates that a SIP device should be reached via a particular prefix, then you should add the device as a neighbor zone with a pattern match equal to the prefix to be used.

The TANDBERG MPS and TANDBERG Content Server (TCS) both support Expressway. They can therefore register directly with a VCS Expressway for firewall traversal.

Registration Overview

Finding a VCS with which to Register

Before an endpoint can register with a VCS, it must determine which VCS it can or should be registering with. This setting is configured on the endpoint, and the process is different for SIP and H.323.

SIP

SIP endpoints must find a SIP Registrar with which to register. The SIP Registrar maintains a record of the endpoint's details against the endpoint's Address of Record (AOR). When a call is received for that AOR, the SIP Registrar refers to the record in order to find the endpoint to which it corresponds. (Note that the same AOR can be used by more than one SIP endpoint at the same time.)

The SIP Registrar will only accept registrations for domains for which it is authoritative.

There are two ways a SIP endpoint can locate a Registrar with which to register: manually or automatically. The option is configured on the endpoint itself under the SIP Server Discovery option (consult your endpoint user guide for how to access this setting).

- If the Server Discovery mode is set to automatic, the endpoint will send a REGISTER message to its SIP Server. This will be forwarded (via DNS if necessary) to the Registrar that is authoritative for the domain with which the endpoint is attempting to register. For example, if an endpoint is attempting to register with a URI of john.smith@example.com, the request will be sent to the Registrar authoritative for the domain example.com.
- If the Server Discovery mode is set to manual, the user must specify the IP address or FQDN of the Registrar with which they wish to register, and the endpoint will attempt to register with that Registrar only.

The VCS is a SIP Server for endpoints in its local zone, and can also act as a SIP Registrar.

- If the VCS is acting as the endpoint's SIP Server and SIP Registrar, when the registration request is received from the endpoint it will be accepted by the VCS and the endpoint will be registered and able to receive inbound calls. See Using the VCS as a SIP Registrar for more information.
- If the VCS is acting as the endpoint's SIP server but is not a SIP Registrar, it will proxy the registration request. See Proxying registration requests for more information.

H.323

There are two ways an H.323 endpoint can locate a VCS with which to register: manually or automatically. The option is configured on the endpoint itself under the Gatekeeper Discovery setting (consult your endpoint manual for how to access this setting).

- If the mode is set to automatic, the endpoint will try to register with any VCS it can find. It does this by sending out a Gatekeeper Discovery Request, to which eligible VCSs will respond.
- If the mode is set to manual, you must specify the IP address of the VCS with which you wish your endpoint to register, and the endpoint will attempt to register with that VCS only.

Preventing automatic registrations

You can prevent H.323 endpoints being able to register automatically with the VCS by disabling Auto Discovery on the VCS. The Auto Discovery setting determines whether the VCS responds to the Gatekeeper Discovery requests sent out by endpoints.

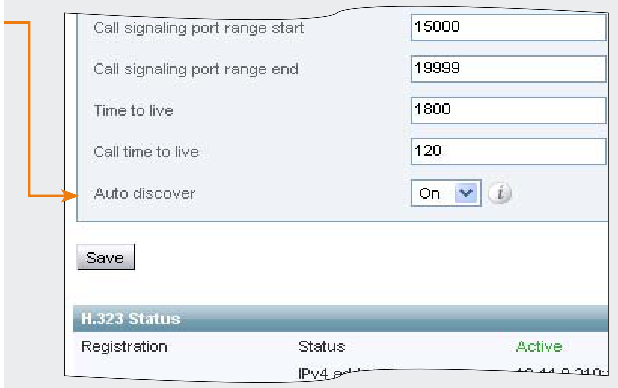
To configure the Auto Discovery setting:

- VCS Configuration > Protocols > H.323.
  You will be taken to the H.323 page.
- H323 Gatekeeper AutoDiscovery

Auto discover

On: The VCS will respond to Gatekeeper discovery requests.

Off: The VCS will reject Gatekeeper discovery requests. H.323 endpoints will be able to register with the VCS only if their Gatekeeper Discovery setting is Manual and they have entered the IP address of the VCS.



Authentication

Authentication Mode

The VCS can be configured to use a username and password-based challenge-response scheme to determine whether it will permit communications from other systems. This process is known as authentication. When Authentication Mode is On, systems attempting to communicate with the VCS, including endpoints attempting to send registration requests to the VCS, must first authenticate with it.

Authentication for Local Registrations

When Authentication Mode is On, endpoints must authenticate with the VCS before they can register. In order to authenticate successfully, the endpoint must supply the VCS with a username. For TANDBERG endpoints using H.323, the username is the endpoint's Authentication ID; for TANDBERG endpoints using SIP it is the endpoint's Authentication Username.

For details of how to configure endpoints with a username and password, please consult the endpoint manual.

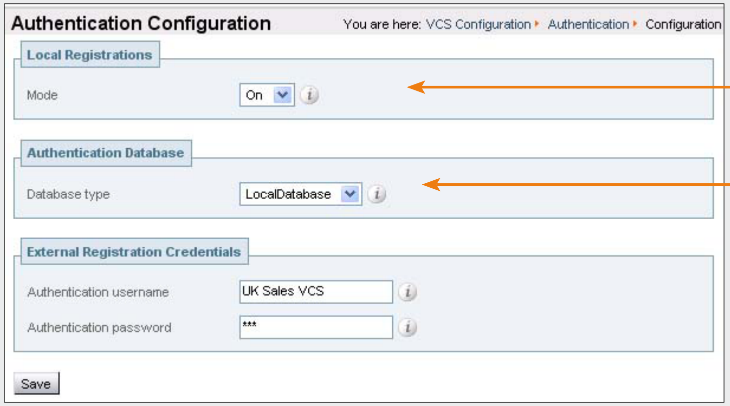
In order to verify the identity of the device, the VCS needs access to a database on which all authentication credential information (usernames, passwords, and other relevant information) is stored. This database may be located either locally on the VCS, or on an LDAP Directory Server. The VCS looks up the endpoint's username in the database and retrieves the authentication credentials for that entry. If the credentials match those supplied by the endpoint, the registration is allowed to proceed.

The VCS supports the ITU H.235 specification [1] for authenticating the identity of H.323 network devices with which it communicates.

Configuring Authentication

To configure the Authentication Mode of the VCS, and the Database it will use:

- VCS Configuration > Authentication > Configuration
  You will be taken to the Authentication Configuration page.
- `xConfiguration Authentication`



Accurate timestamps play an important part in authentication, helping to guard against replay attacks. For this reason, if you are using authentication, both the VCS and the endpoints must use an NTP server to synchronize their system time. See the NTP section for information on how to configure this for the VCS.

Mode

Determines whether systems attempting to communicate with the VCS must authenticate with it first.

On: For H.323, any credentials in the message are checked against the authentication database. The message is allowed if the credentials match, or if there are no credentials in the message. For SIP, any messages originating from an endpoint in a local domain will be authenticated.

Off: no authentication is required for endpoints.

The default is Off.

Database type

Determines which database the VCS will use during authentication.

LocalDatabase: the local database is used. You must configure the Local database to use this option.

LDAP: A remote LDAP database is used. You must configure the LDAP server to use this option.

The default is LocalDatabase.

If the VCS is a traversal server, you must ensure that each traversal client's authentication credentials are entered into the selected database.

Registration Control

Authentication

About External Registration Credentials

The VCS may be required to authenticate itself with another system. For example, when the VCS is forwarding an invite from an endpoint to another VCS, that other system may have authentication enabled and will therefore require your local VCS to provide it with a username and password.

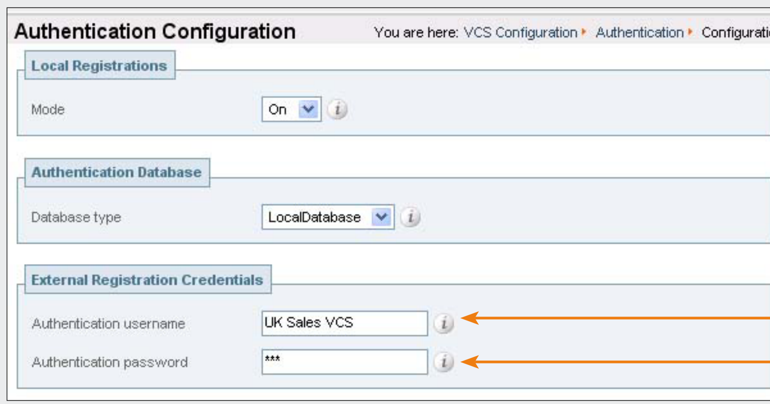
Additionally, traversal clients must always successfully authenticate with traversal servers before they can connect.

The username and password that your VCS provides when authenticating with other systems is configured under the External Registration Credentials section of the Authentication Configuration page.

Configuring External Registration Credentials

To configure Authentication options:

- VCS Configuration > Authentication > Configuration
  You will be taken to the Authentication Configuration page (shown below).
- xConfiguration Authentication



Authentication username

The Authentication Username is the name that the VCS uses when authenticating with other systems.

Authentication password

Specifies the password to be used by the VCS (in conjunction with the Authentication username) when the VCS is authenticating with other systems.

Authentication Databases

Alias Origin Setting

This setting determines the alias(es) with which the endpoint will attempt to register. The options are as follows:

LDAP

The alias(es) presented by the endpoint will be used as long as they are listed in the LDAP database for the endpoint's username.

- If an endpoint presents an alias that is listed in the LDAP database, it will be registered with that alias.
- If more than one alias is listed in the LDAP database for that username, the endpoint will be registered with only those aliases that it has presented.
- If an endpoint presents an alias that is not in the LDAP database, it will not be registered with that alias.
- If an endpoint presents more than one alias but none are listed in the LDAP database, it will not be allowed to register.
- If no aliases are presented by the endpoint, it will be registered with all the aliases listed in the LDAP database for its username. (This is to allow for MCUs which additively register aliases for conferences, for example the TANDBERG MPS (J4.0 and later) which registers ad-hoc conferences.) (This applies to H.323 only).
- If no aliases are listed in the LDAP database for the endpoint's username, then the endpoint will be registered with all the aliases it presented.

Combined

The alias(es) presented by the endpoint will be used in addition to any that are listed in the LDAP database for the endpoint's username. In other words, this is the same as for LDAP, with one exception:

- If an endpoint presents an alias that is not in the LDAP database, it will be allowed to register with that alias.

Endpoint

The alias(es) presented by the endpoint will be used; any in the LDAP database will be ignored.

- If no aliases are presented by the endpoint, it will not be allowed to register.

Authentication using an LDAP Server

If the VCS is using an LDAP server for authentication, the process is as follows:

1. The endpoint presents its username and authentication credentials (these are generated using its password) to the VCS, and the alias(es) with which it wishes to register
2. The VCS looks up the username in the LDAP database and obtains the authentication and alias information for that entry.
3. If the authentication credentials match those supplied by the endpoint, the registration will continue.

The VCS will then determine which alias(es) the endpoint will be allowed to attempt to register with, based on the alias origin setting. For H.323 endpoints, you can use this setting to override the aliases presented by the endpoint with those in the H.350 directory, or you can use them in addition to the endpoint's aliases. For SIP endpoints, you can use this setting to reject a registration if the endpoint's AOR does not match that in the LDAP database.

Configuring the LDAP Server Directory

The directory on the LDAP server should be configured to implement the ITU H.350 specification [2] to store credentials for devices with which the VCS communicates. The directory should also be configured with the aliases of endpoints that will register with the VCS.

For instructions on how to configure common LDAP servers, see the Appendix LDAP Configuration.

Securing the LDAP Connection with TLS

The traffic between the VCS and the LDAP server can be encrypted using Transport Layer Security (TLS).

To use TLS:

- LDAP Encryption must be set to TLS
- the LDAP server must have a valid certificate installed, verifying its identity
- The VCS must trust the certificate installed on the LDAP server.

TLS can be difficult to configure, so we recommend that you confirm that your LDAP database is working correctly before you attempt to secure the connection with TLS. We also recommend that you use a third party LDAP browser to verify that your LDAP server is correctly configured to use TLS.

For information on how to configure the VCS to trust the certificate installed on the LDAP server, see the Security section.

Registration Control

Authentication Databases

Configuring LDAP Server settings

To configure the settings for accessing the LDAP server:

- VCS Configuration > Authentication > LDAP > Configuration.
  You will be taken to the LDAP Configuration page.
- xConfiguration LDAP
- xConfiguration Authentication LDAP

Alias origin

Determines the source of the alias(es) with which the endpoint will be registered.

LDAP: The aliases listed in the LDAP database for the endpoint's username will be used; those presented by the endpoint will be ignored.

Endpoint: The aliases presented by the endpoint will be used; any in the LDAP database will be ignored.

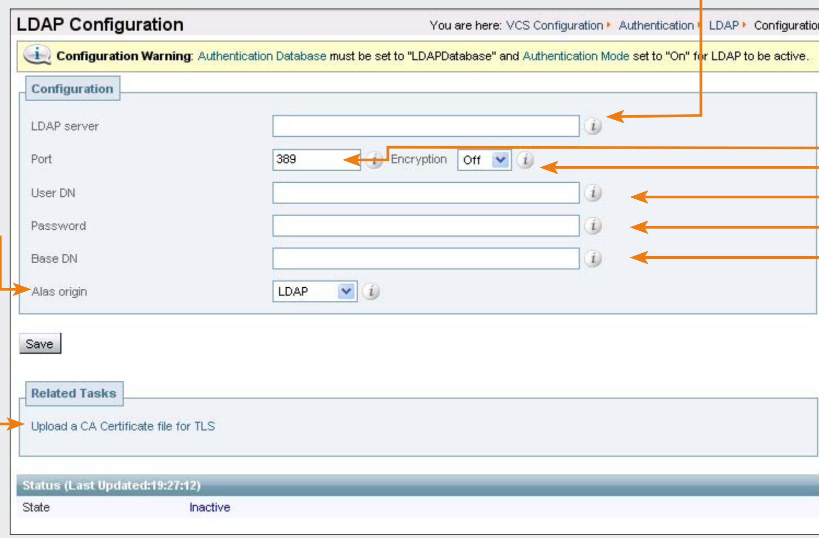
Combined: The endpoint will be registered both with the aliases which it has presented and with those configured in the LDAP database.

The default is LDAP.

Upload a CA Certificate file for TLS

Clicking here will take you to the Security page, where you can upload a file that contains the trusted CA certificate for the LDAP server. This is required if the connection between the VCS and the LDAP server is encrypted.

For more information on how to configure the VCS to trust the certificate installed on the LDAP server, see the Security section.



LDAP Server

The IP address or FQDN (or server address, if a DNS Domain Name has also been configured) of the LDAP server.

Port

The IP port of the LDAP server.

The default is 389.

Encryption

Determines whether the connection to the LDAP server will be encrypted. (For more information on configuring encryption, see Securing the LDAP connection with TLS.)

TLS: TLS Encryption will be used for the connection with the LDAP server.

Off: No encryption will be used.

The default is Off.

UserDN

The user distinguished name to be used by the VCS when binding to the LDAP server.

Password

The password to be used by the VCS when binding to the LDAP server.

Base DN

The area of the directory on the LDAP server to be searched for the credential information.

This should be specified as the Distinguished Name (DN) in the LDAP directory under which the H.350 objects reside.

Registration Control

Authentication Databases

Authentication using a Local Database

The local database is included as part of your VCS system. It consists of a list of usernames and passwords, which you add via the web interface and/or the CLI. The database can hold up to 2500 entries.

Configuring the Local Database

To manage entries in the Local Database:

- VCS Configuration > Authentication > Local Database.
  You will be taken to the Credentials page.
- xConfiguration Authentication Credential
- xCommand CredentialAdd
- xCommand CredentialDelete

New

Select New to add a new entry to the Local Database. You will be taken to the Create Credential page.

Name

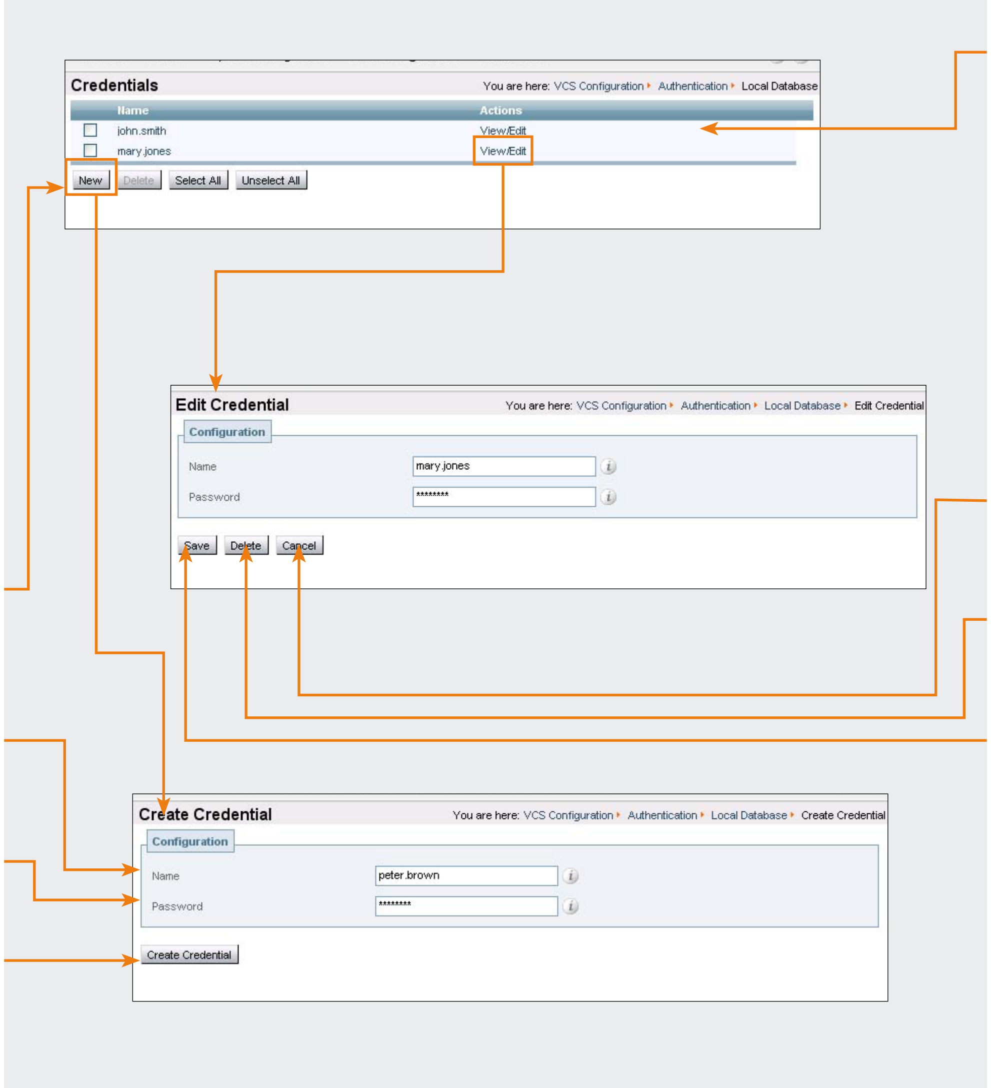
The username used by the endpoint when authenticating with the VCS.

Password

The password used by the endpoint when authenticating with the VCS.

Create Credential

Select Create Credential to add the new entry to the Local Database and return to the Credentials page.



Credentials

The Credentials page shows all the existing entries in the Local Database.

You can sort these entries by clicking on the Name column heading.

View/Edit

Select View/Edit to add a make changes to an existing entry. You will be taken to the Edit Credential page.

Cancel

Returns you to the Credentials page without saving your changes.

Delete

Removes the entry from the Local Database and returns you to the Credentials page.

Save

Saves the changes you have made.

The same credentials can be used by more than one endpoint - you do not need to have a separate entry in the database for each endpoint.

Registration Control

Registering Aliases

About Alias Registration

Once the authentication process (if required) has been completed, the endpoint will then attempt to register its alias(es) with the VCS.

Attempts to Register using an Existing Alias

An endpoint may attempt to register with the VCS using an alias that is already registered to the system. How this is managed depends on how the VCS is configured and whether the endpoint is SIP or H.323.

SIP

A SIP endpoint will always be allowed to register using an alias that is already in use from another IP address. When a call is received for this alias, all endpoints registered using that alias will be called simultaneously. This SIP feature is known as "forking".

H.323 Alias Registration

When registering, the H.323 endpoint presents the VCS with one or more of the following:

- one or more H.323 IDs
- one or more E.164 aliases
- one or more URIs.

Users of other registered endpoints can then call the endpoint by dialing any of these aliases.

We recommended that you register your H.323 endpoints using a URI. This facilitates interworking between SIP and H.323, as SIP endpoints register using a URI as standard.

We recommended that you do not use aliases that reveal sensitive information. Due to the nature of H.323, call setup information is exchanged in an unencrypted form.

SIP Alias Registration

When registering, the SIP endpoint presents the VCS with its contact address (IP address) and logical address (Address of Record). The logical address is considered to be its alias, and will generally be in the form of a URI.

H.323

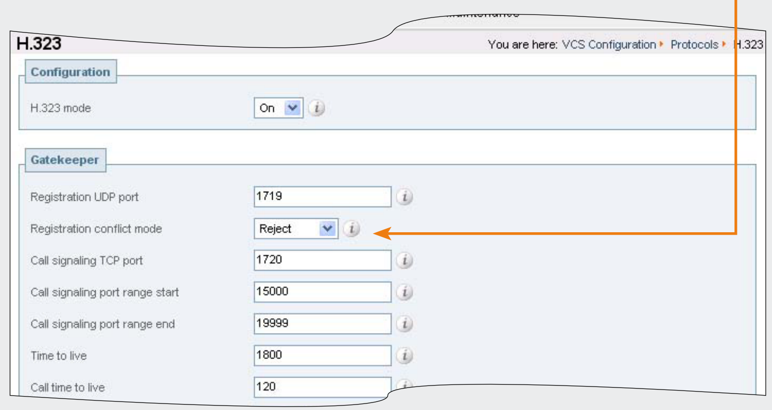
An H.323 endpoint may attempt to register with the VCS using an alias that has already been registered on the VCS from another IP address. The reasons for this could include:

- two endpoints at different IP addresses are attempting to register using the same alias
- a single endpoint has previously registered using a particular alias. The IP address allocated to the endpoint, or the port the endpoint uses to communicate with the VCS, then changes, and the endpoint is attempting to re-register using the same alias.

You can determine how the VCS will behave in this situation by configuring the Registration Conflict Mode.

To configuring the Registration Conflict Mode:

- VCS Configuration > Protocols > H.323. You will be taken to the H.323 page.
- xConfiguration H323 Gatekeeper Registration ConflictMode



Registration conflict mode

Determines what will happen when an H.323 endpoint attempts to register using an alias that has already been registered from another IP address.

Reject: The registration from the new IP address will be rejected. This is useful if your priority is to prevent two users registering with the same alias.

Overwrite: The existing registration will be overwritten using the new IP address. This is useful if your network is such that endpoints are often allocated new IP addresses, because it will prevent unwanted registration rejections.

The default is Reject.

Registration Control

Allow and Deny Lists

About Allow and Deny Lists

When an endpoint attempts to register with the VCS it presents a list of aliases. You can control which endpoints are allowed to register by setting the Restriction Policy to AllowList or DenyList and then including any one of the endpoint's aliases on the Allow List or the Deny list as appropriate. Each list can contain up to 2,500 entries. When an endpoint attempts to register, each of its aliases is compared with the patterns in the relevant list to see if it matches. Only one of the aliases needs to appear in the Allow List or the Deny List for the registration to be allowed or denied.

For example, If the Registration Restriction policy is set to DenyList and an endpoint attempts to register using three aliases, one of which matches a pattern on the Deny list, that endpoint's registration will be denied. Likewise, if the Registration Restriction policy is set to AllowList, only one of the endpoint's aliases needs to match a pattern on the Allow list for it to be allowed to register using all its aliases.

Patterns and Pattern Types

Entries on the Allow List and Deny List are a combination of Pattern and Type. The Pattern specifies the string to be matched; the Type determines whether that string;

- must match the Pattern exactly (Exact)
- must appear at the start of the alias (Prefix)
- must appear at the end of the alias (Suffix)
- is in the form of a Regular Expression (Regex).

Removing existing registrations

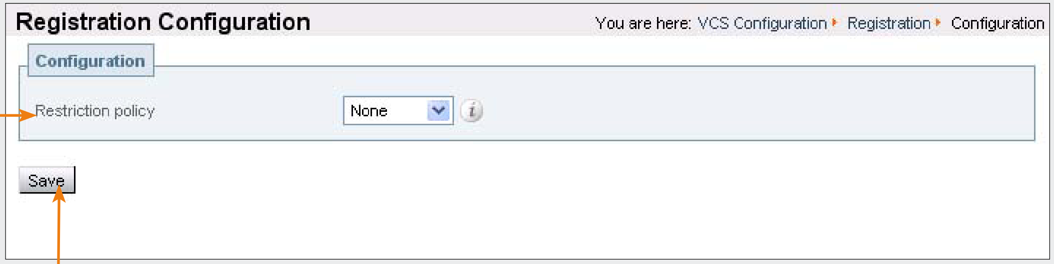
Once an Allow List or Deny List has been activated, it will be used to control all registration requests from that point forward. However, any existing registrations will remain in place, even if the new list would otherwise block them. For this reason we recommend that you manually remove all existing unwanted registrations after you have implemented an Allow List or Deny List.

To manually remove a registration; navigate to Status > Registrations, select the registration(s) you wish to remove, and click Unregister.

Activating use of Allow or Deny Lists

To activate the use of Allow or Deny lists to determine which aliases are allowed to register with the VCS:

- VCS Configuration > Registration > Configuration.
  You will be taken to the Registration Configuration page.
- `xConfiguration Registration RestrictionPolicy`



Restriction policy

Specifies the policy to be used when determining which endpoints may register with the VCS.

None: Any endpoint may register.

AllowList: Only those endpoints with an alias that matches an entry in the Allow List may register.

DenyList: All endpoints may register, unless they match an entry on the Deny List.

The default is None.

Save

Click here to save your changes.

Allow Lists and Deny Lists are mutually exclusive: only one may be in use at any given time.

Allow and Deny lists

Managing Entries in the Allow List

To view and manage the entries in the Allow List:

- VCS Configuration > Registration > Allow List.
  You will be taken to the Registration Allow List page.
- xCommand AllowListAdd
- xConfiguration Registration AllowList

New

Click here to add a new entry to the Allow List. You will be taken to the Create Allow Pattern page.

Pattern

Enter the pattern you wish to add to the Allow List.

Type

Select the way in which the Pattern must match the alias for the registration to be allowed. Options are:

Exact: the alias must match the Pattern exactly.

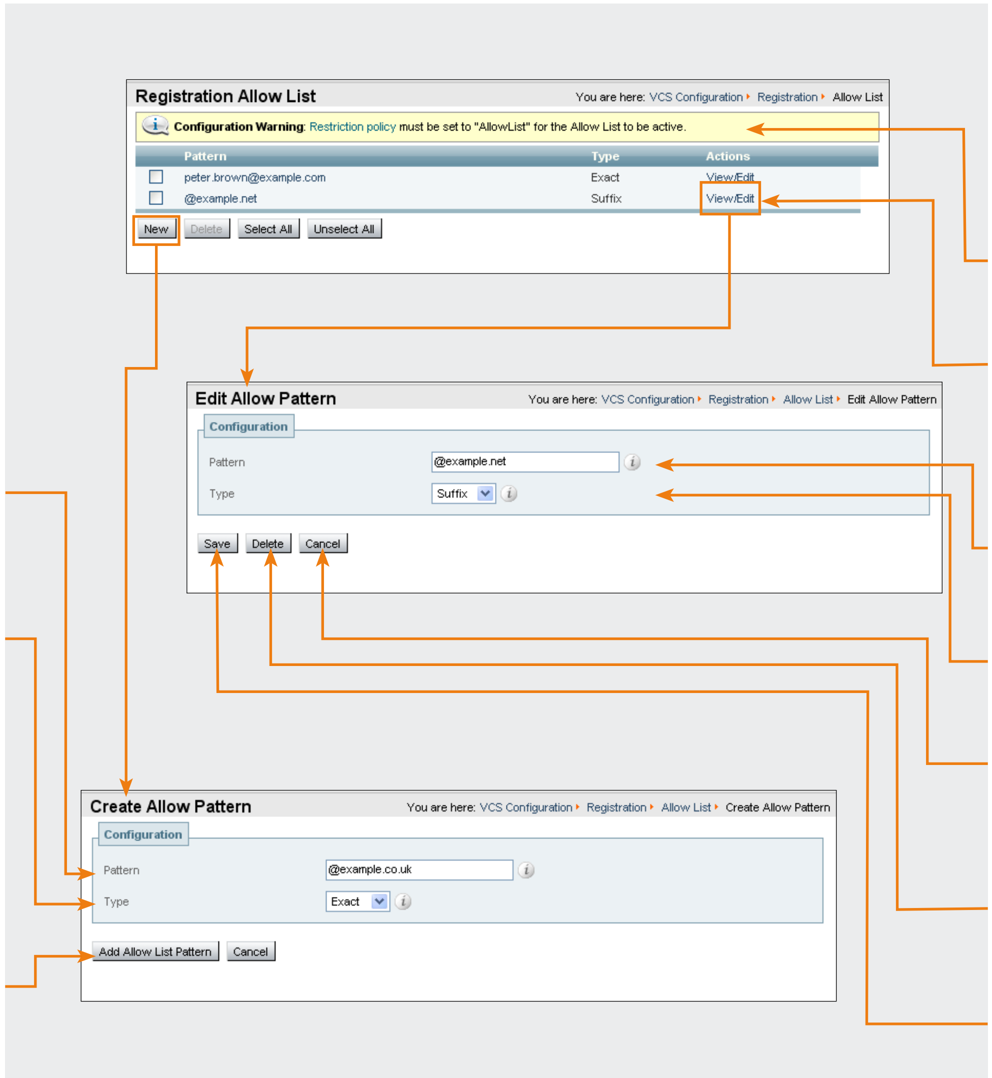
Prefix: the alias must begin with the Pattern.

Suffix: the alias must end with the Pattern.

Regex: the Pattern is a regular expression. See Regular Expression Reference for further information.

Add Allow List Pattern

Click here to save the entry and return to the Registration Allow List page.



Registration Allow List

This page shows all the existing entries in the Allow List.

You can sort these entries by clicking on the relevant column heading.

This warning is a reminder that you must set the restriction policy to Allow List (VCS Configuration > Registration > Configuration) in order for it to be activated.

View/Edit

Select View/Edit to make changes to an existing entry. You will be taken to the Edit Allow Pattern page.

Pattern

Edit the pattern.

Type

Edit the type.

Cancel

Select Cancel to return to the Registration Allow List page without saving your changes.

Delete

Select Delete to remove the registration from the list.

Save

Select Save to save your changes.

Allow and Deny lists

Managing Entries in the Deny List

To view and manage the entries in the Deny List:

- VCS Configuration > Registration > Deny List.
  You will be taken to the Registration Deny List page.
- xCommand DenyListAdd
- xConfiguration Registration DenyList

New

Click here to add a new entry to the Deny List. You will be taken to the Create Deny Pattern page.

Pattern

Enter the pattern you wish to add to the Deny List.

Type

Select the way in which the Pattern must match the alias for the registration to be denied. Options are:

Exact: the alias must match the Pattern exactly.

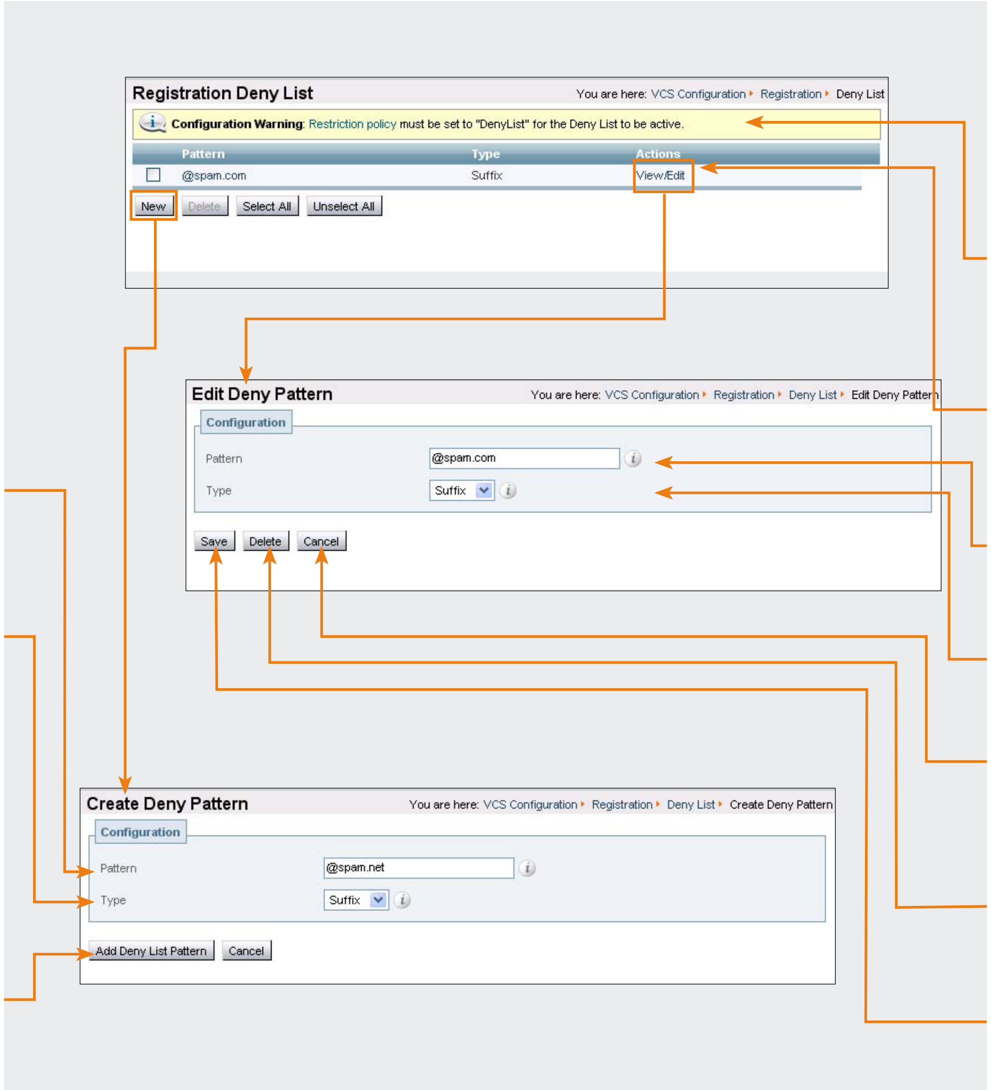
Prefix: the alias must begin with the Pattern.

Suffix: the alias must end with the Pattern.

Regex: the Pattern is a regular expression. See Regular Expression Reference for further information.

Add Deny List Pattern

Click here to save the entry and return to the Registration Deny List page.



Registration Deny List

This page shows all the existing entries in the Deny List.

You can sort these entries by clicking on the relevant column heading.

This warning is a reminder that you must set the restriction policy to Deny List (VCS Configuration > Registration > Configuration) in order for it to be activated.

View/Edit

Select View/Edit to make changes to an existing entry. You will be taken to the Edit Deny Pattern page.

Pattern

Edit the pattern.

Type

Edit the type.

Cancel

Select Cancel to return to the Registration Deny List page without saving your changes.

Delete

Select Delete to remove the registration from the list.

Save

Select Save to save your changes.

Zones and Neighbors

This section begins with an overview of all the different types of subzones and zones and how these fit into the overall structure of your video communication network.

It then provides information on the pages that appear under the Local Zone, Zones and Alternates sub-menus of the VCS Configuration menu.

These pages allow you to:

- configure the VCS's Local Zone (which is made up of subzones, including the Traversal Subzone and Default Subzone)
- create and configure external zones to communicate with other systems and endpoints, including other VCSs, Gatekeepers, Border Controllers or SIP devices, and endpoints contactable via DNS or ENUM dialing.
- create VCS Clusters to increase the capacity of your local zone, and for resiliency.



About your Video Communications Network

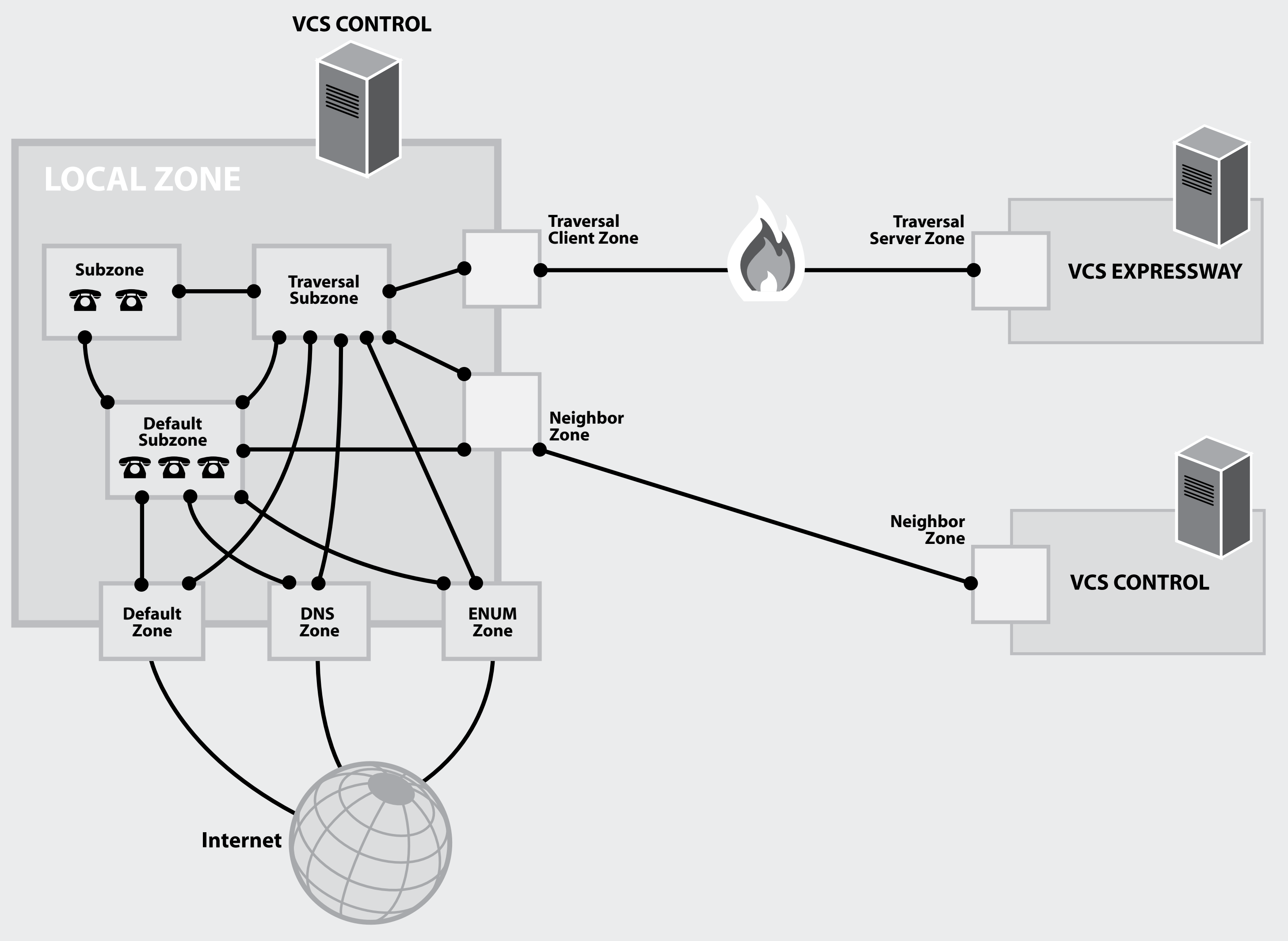
The most basic implementation of a TANDBERG video communications network is a single VCS connected to the internet with one or more endpoints registered to it. However, depending on the size and complexity of your enterprise the VCS may be part of a network of endpoints, other VCSs and other network infrastructure devices, with one or more firewalls between it and the internet. In such situations you may wish to apply restrictions to the amount of bandwidth used by and between different parts of your network.

This section will give you an overview of the different parts of the video communications network and the ways in which they can be connected. This information should allow you to configure your VCS to best suit your own infrastructure.

Example Network Diagram

The diagram opposite shows the different components of a VCS (i.e. subzones and zones) and how they interrelate. Using a VCS Control as the example Local Zone, it shows that it is made up of a number of subzones which are all connected by links. The Local Zone is also connected to external VCSs and to the internet via different types of zones.

All these components are described in more detail in the sections that follow.



Local Zone and Subzones

Overview

The collection of all endpoints, gateways, MCUs and Content Servers registered with the VCS make up its Local Zone.

The Local Zone is divided into subzones. These include an automatically created Default Subzone and up to 100 manually configurable subzones. Each manually configured subzone specifies a range of IP addresses. When an endpoint registers with the VCS it is allocated to the appropriate subzone based on its IP address. If the endpoint's IP address does not match any of the subzones, it is assigned to the Default Subzone. The Local Zone may be independent of network topology, and may be comprised of multiple network segments.

The VCS also has two special types of subzones. The first is the Traversal Subzone, which is always present (see the Traversal Subzone section for more information). The second is the Cluster Subzone, which is only present when your VCS is part of a cluster (see the Clustering section for more information).

Configuring the Local Zone and its Subzones

Bandwidth Management

The Local Zone's subzones exist for the purposes of bandwidth management. Once you have set up your subzones you can apply bandwidth limits to:

- individual calls between two endpoints within the subzone
- individual calls between an endpoint within the subzone and another endpoint outside of the subzone
- the total of calls to or from endpoints within the subzone.

For full details of how to create and configure subzones, and apply bandwidth limitations to subzones including the Default Subzone and Traversal Subzone, see the section on Bandwidth Control.

Local Zone Matches

One of the functions of the VCS is to route a call received from a locally registered endpoint or external zone to its appropriate destination. Calls are routed based on the address or alias of the destination endpoint.

When searching for a destination endpoint, the VCS will search its Local Zone and external zones. You can prioritize the order in which these zones are searched, and filter the search requests sent to each zone, based on the address or alias being searched for. This allows you to reduce the potential number of search requests sent to the Local Zone and out to external zones, and speed up the search process.

For further information on how to configure the Local Zone Matches and the overall process for searching zones, see the Zone Searching and Transforming section.

The ability to include the Local Zone when prioritizing zone searches is a new feature in VCS version X3.0. Prior to this version, the Local Zone was always searched before any external zones.

Traversal Subzone

The Traversal Subzone is a conceptual subzone; no endpoints can be registered to it, but all traversal calls (i.e. calls for which the VCS is taking the media in addition to the signaling) will pass through it. The Traversal Subzone exists in order to allow you to control the amount of bandwidth used by traversal calls, as these can be particularly resource-intensive.

What are traversal calls?

The following types of calls require the VCS to take the media. They are classified as traversal calls and will always pass through the Traversal Subzone:

- Firewall traversal calls
- calls that are gatewayed (interworked) between H.323 and SIP
- calls that are gatewayed (interworked) between IPv4 and IPv6
- for VCSs with Dual Network Interfaces enabled, calls that are inbound from one LAN port and outbound on the other
- a SIP to SIP call when one of the participants is behind a NAT.

All such calls will require a traversal call licence each time they pass through the Traversal Subzone.

STUN Relays also consume traversal call licences (three relays take one licence) but they do not actually pass through the Traversal Subzone.

Configuring the Traversal Subzone Ports

The VCS allows you to configure the range of ports to be used for the media in traversal calls. A single traversal call can consist of up to 5 types of media (audio, video, far end camera control, dual streams and BFCP) and each type of media may require a pair of ports – for example, audio and video each require one port for RTP, and one for RTCP. Separate pairs of ports are required for the inbound and outbound portions of a call. A single traversal call can therefore take up to 20 ports.

The default range for the ports to be used for media is 50000 - 51119 UDP, but these can be changed to anywhere between 1024 and 65533. Ports are allocated from this range in pairs, the first of each being even. Therefore the range must start with an even number and end with an odd number.

To configure the ports used for media in traversal calls:

- VCS Configuration > Local Zone > Traversal Subzone
- `xConfiguration Traversal Media Port Start`
- `xConfiguration Traversal Media Port End`

You must ensure that the port range is large enough to support the maximum number of traversal calls available on your VCS. A single traversal call can take up to 20 ports (5 pairs in each direction). So for example, if your VCS is licensed for 5 traversal calls you must ensure that the range of ports configured for traversal media is at least 100. If you add extra traversal calls to your system, you must also ensure that the range of ports available is sufficient.

Zones

About Zones

A zone is a collection of endpoints, either all registered to a single system (e.g. TANDBERG VCS, gatekeeper, or TANDBERG Border Controller), or of a certain type such as ENUM or DNS. The use of zones enables you to:

- use links to determine whether calls can be made between your local subzones and these other zones
- manage the bandwidth of calls between your local subzones and endpoints in other zones
- easily search for aliases that are not registered locally
- apply transforms to aliases before searching for them.

Your VCS allows you to configure up to 200 zones of 5 different types. It also has a non-configurable Default Zone.

Neighbor Zone

A Neighbor zone could be a collection of endpoints registered to another system (e.g. VCS, gatekeeper, or Border Controller), or it could be a SIP device. The other system or SIP device is referred to as a neighbor. Neighbors can be part of your own enterprise network, part of a separate network, or even stand-alone systems.

You create a neighbor relationship with the other system by adding it as a neighbor zone on your local VCS. Once you have added it, you can:

- query the neighbor about its endpoints
- apply transforms to any requests before they are sent to the neighbor
- control the bandwidth used for calls between your local VCS and the neighbor zone.

Neighbor zone relationships are one-way; adding another system to your VCS as a neighbor does not mean that your VCS will also be a neighbor of that other system. In such a situation, your VCS will know about and be able to query the other system, but the other system will not know about or be able to query your VCS. However, inbound calls will be identified as coming from that neighbor if the source IP address matches.

Traversal Client Zone

In order to be able to traverse a firewall, the VCS must be neighbored with a traversal server (for example a TANDBERG VCS Expressway or a TANDBERG Border Controller).

In this situation your local VCS is a traversal client, so you neighbor with the traversal server by creating a traversal client zone on your local VCS. You then configure the client zone with details of the corresponding zone on the traversal server. (The traversal server must also be configured with details of the VCS client zone.)

Once you have neighbored with the traversal server you can:

- use the neighbor as a traversal server
- query the traversal server about its endpoints
- apply transforms to any queries before they are sent to the traversal server
- control the bandwidth used for calls between your local VCS and the traversal server.

Traversal Server Zone

A VCS Expressway is able to act as a traversal server, providing firewall traversal on behalf of traversal clients (for example, VCS Controls or gatekeepers).

In order to act as a traversal server, the VCS Expressway must have a special type of two-way neighbor relationship with each traversal client. To do this, you create a traversal server zone on your local VCS Expressway and configure it with the details of the corresponding zone on the traversal client. (The client must also be configured with details of the VCS Expressway.)

Once you have neighbored with the traversal client you can:

- provide firewall traversal services to the traversal client
- query the traversal client about its endpoints
- apply transforms to any queries before they are sent to the traversal client
- control the bandwidth used for calls between your local VCS and the traversal client.

Traversal client-server zone relationships are two-way; in order for firewall traversal to work, the traversal server and the traversal client must each be configured with the other's details. (See Quick Guide to VCS Traversal Client - Server Configuration for more information.) The client and server will then be able to query each other.

Zones

ENUM Zone

ENUM zones allow you to locate endpoints via an ENUM lookup. You can create one or more ENUM zones based on the ENUM DNS suffix used and/or by pattern matching of the endpoints' aliases.

Once you have configured one or more ENUM zones, you can:

- apply transforms to alias search requests directed to that group of endpoints
- control the bandwidth used for calls between your local VCS and each group of ENUM endpoints.

See ENUM Dialing for more information on the use of ENUM zones.

DNS Zone

DNS zones allow you to locate endpoints via a DNS lookup. You can create one or more DNS zones based on pattern matching of the endpoints' aliases.

Once you have configured one or more DNS zones, you can:

- apply transforms to alias search requests directed to that group of endpoints
- control the bandwidth used for calls between your local VCS and each group of DNS endpoints.

Default Zone

Any incoming calls from endpoints that are not recognized as belonging to any of the existing configured zones are deemed to be coming from the Default Zone.

The VCS comes pre-configured with the Default Zone and default links between it and both the Default Subzone and the Traversal Subzone.

The purpose of the Default Zone is to allow you to manage incoming calls from unrecognized endpoints to the VCS. You can do this by:

- deleting the default links. This will prevent any incoming calls from unrecognized endpoints
- applying pipes to the default links. This will allow you to control the bandwidth consumed by incoming calls from unrecognized endpoints.

The default links can be reinstated at any time via the command:
`xCommand DefaultLinksAdd`

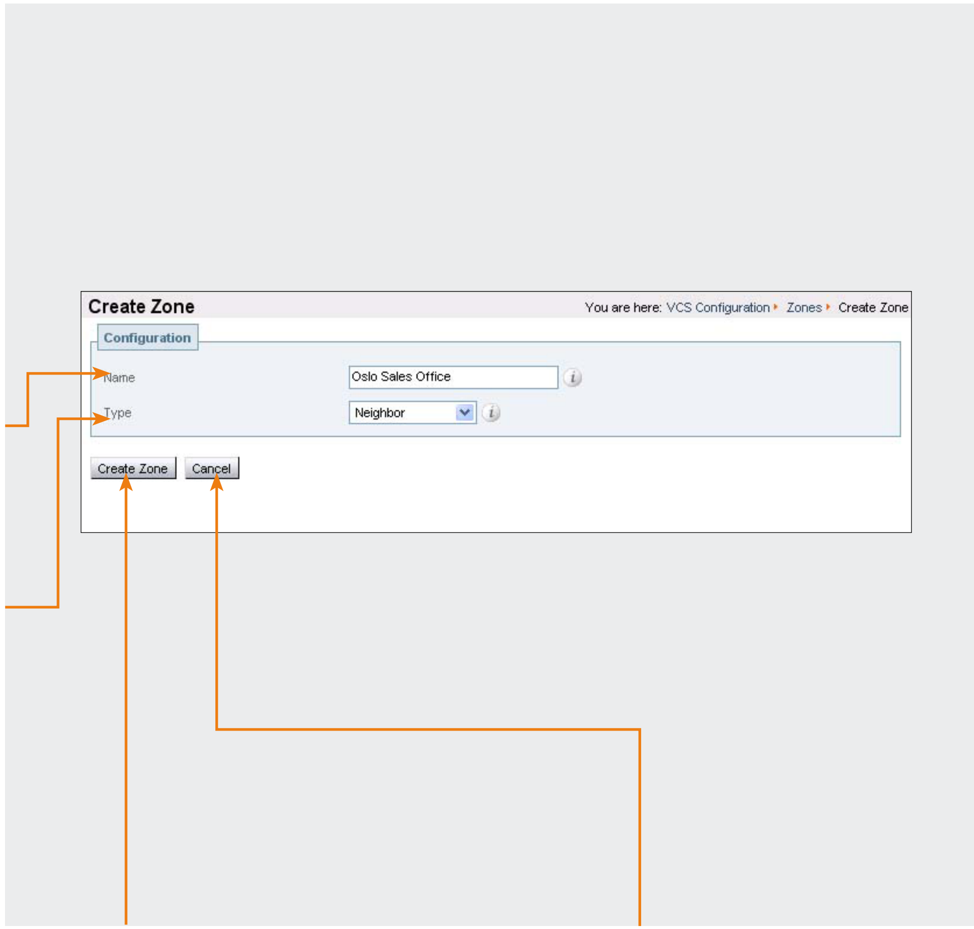
Zones

Adding Zones

In order to neighbor with another system (e.g. VCS, gatekeeper or Border Controller) or create an ENUM or DNS zone, you must add a new zone on the local VCS. When adding a new zone you will be asked to specify its Type; this will determine which configuration options will then be available.

To create a new zone:

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click New.
  You will be taken to the Create Zone page.
- xCommand ZoneAdd



Name

Enter the name you wish to give to this zone. The name acts as a unique identifier, allowing you to distinguish between zones of the same type.

Type

From the Type drop-down menu, select the type of zone you wish to add.

Neighbor: the new zone will be a connection to a neighbor of the local VCS.

TraversalClient: the local VCS is a traversal client of the new zone, and there is a firewall between the two.

TraversalServer: the local VCS is a traversal server for new zone, and there is a firewall between the two.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Once the zone has been created, the Type cannot be changed.

Create Zone

Click here to create the zone. You will be taken directly to the Edit Zone page.

Cancel

Click here to return to the Zones page without creating the zone.

Configuring Zones

Once you have created a new zone on the local VCS you must configure it appropriately. For traversal server zones, traversal client zones and neighbor zones this will include providing information about the neighbor system such as IP address and ports.

Zones are configured via the Edit Zone page. You will be taken to this page automatically upon creation of a new zone. To access this page for an existing zone:

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zone page.
- xConfiguration Zones Zone [1..200]

The sections that follow describe the configuration options available for each zone type.

Configuring Zones - All Types

Name

Assigns a name to the zone. The name acts as a unique identifier, allowing you to distinguish between zones of the same type.

Type

Determines the nature of the zone:

Neighbor: the new zone will be a connection to a neighbor of the local VCS.

TraversalClient: the local VCS is a traversal client of the new zone, and there is a firewall between the two.

TraversalServer: the local VCS is a traversal server for new zone, and there is a firewall between the two.

ENUM: the new zone contains endpoints discoverable by ENUM lookup.

DNS: the new zone contains endpoints discoverable by DNS lookup.

Once the zone has been created, the Type cannot be changed.

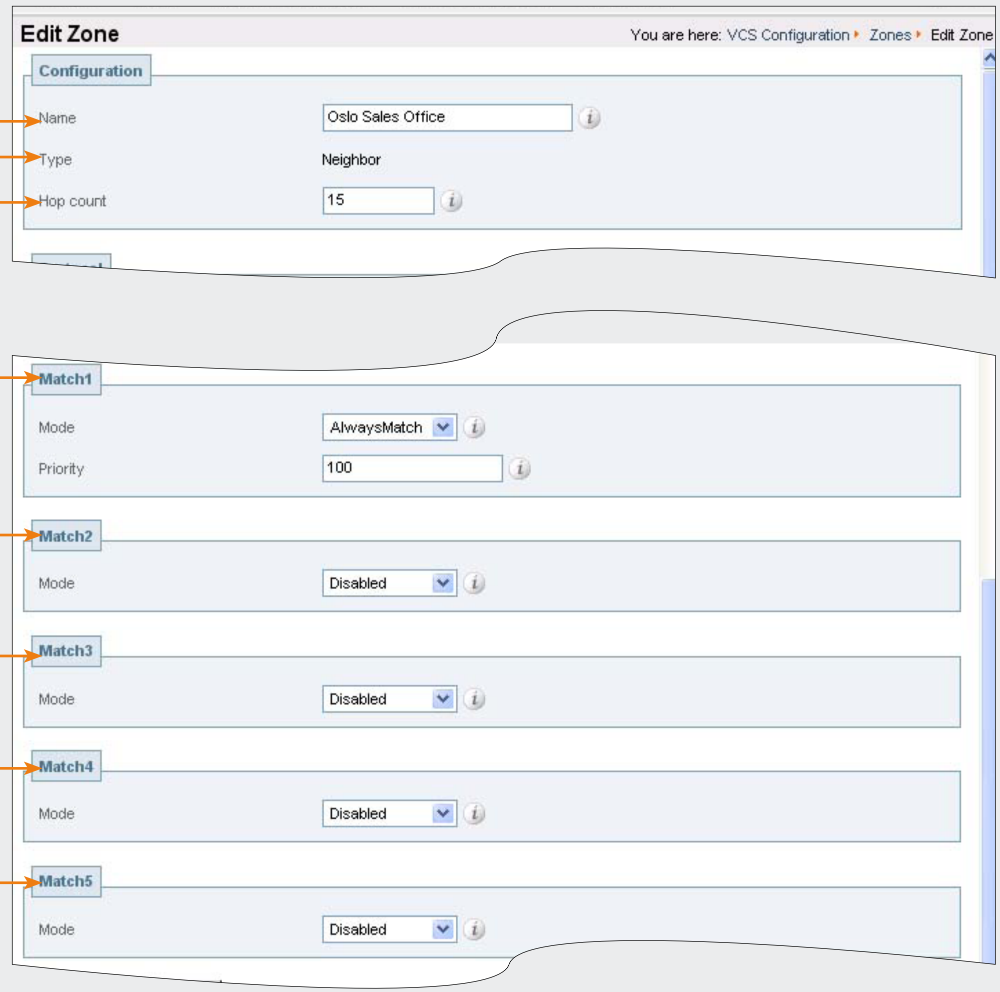
Hop count

The hop count is the number of times a request will be forwarded to a neighbor gatekeeper or proxy (see Hop Counts for more information). This field specifies the hop count to be used when sending an alias search request to this particular zone.

If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

Match1 - Match5

The Match sections allow you to configure when and how search requests will be sent to this zone, and also whether any transforms will be applied to aliases being searched for in this zone. These features are described in full in the section Zone searching and alias transforming.



Configuring Neighbor Zones

SIP mode

Determines whether SIP calls will be allowed to and from the neighbor zone.

SIP port

Specifies the port on the neighbor system to be used for SIP calls from the local VCS.

This must be the same port number as that configured on the neighbor system as its SIP TCP, SIP TLS or SIP UDP port (depending on which SIP transport mode is in use).

SIP transport

Determines which transport type will be used for SIP calls to and from the neighbor zone.

H.323 mode

Determines whether H.323 calls will be allowed to and from the neighbor zone.

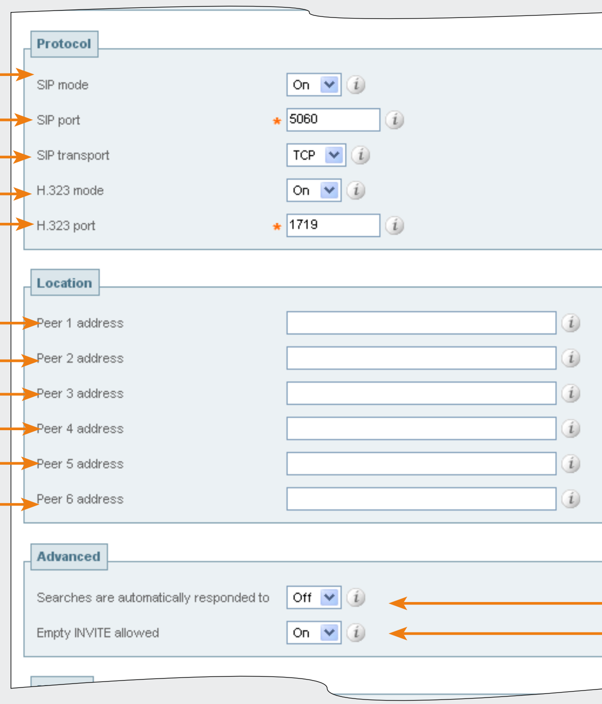
H.323 port

Specifies the port on the neighbor system to be used for H.323 calls from the local VCS.

This must be the same port number as that configured on the neighbor system as its H.323 UDP port. If the neighbor is another VCS, this will be the port found under VCS Configuration > Protocols > H.323 in the Registration UDP Port field.

Peer 1 to Peer 6 address

The IP Address or FQDN of the neighbor system. If the neighbor is a VCS cluster, this includes all of its Peers. See the section Neighboring the Local VCS to a Cluster for more information.



Searches are automatically responded to

Determines what happens when the VCS receives a SIP search that originated as an H.323 search, destined for this zone. The default is Off.

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

This option should normally be left as the default Off. However, some systems such as Microsoft OCS 2007 will not accept SIP OPTION messages, so for these zones this should be set to On. If you do change this to On, you must also configure pattern matches to ensure that only those searches that actually match endpoints in this zone are responded to. If you do not, the search will not continue to other lower-priority zones, and the call will be forwarded to this zone even if it cannot support it.

Refer to the relevant TANDBERG VCS Deployment Guide for full details on how to configure these advanced options for specific systems.

Empty INVITE allowed

Determines whether the VCS will generate a SIP INVITE message with no SDP to send to this zone. INVITES with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323. The default is On.

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.

In most cases this option should normally be left as the default On. However, some systems such as Microsoft OCS 2007 will not accept invites with no SDP, so for these zones this should be set to Off.

Refer to the relevant TANDBERG VCS Deployment Guide for full details on how to configure these advanced options for specific systems.

Configuring Traversal Client Zones

Authentication username

Traversal clients must always authenticate with traversal servers by providing their authentication username and password.

The client's authentication username is shown here for reference, to make it easier to configure the corresponding zone on the traversal server.

The authentication username is a system-wide setting that is set via VCS Configuration > Authentication > Configuration.

H.323 mode

Determines whether H.323 calls will be allowed to and from the traversal server.

H.323 protocol

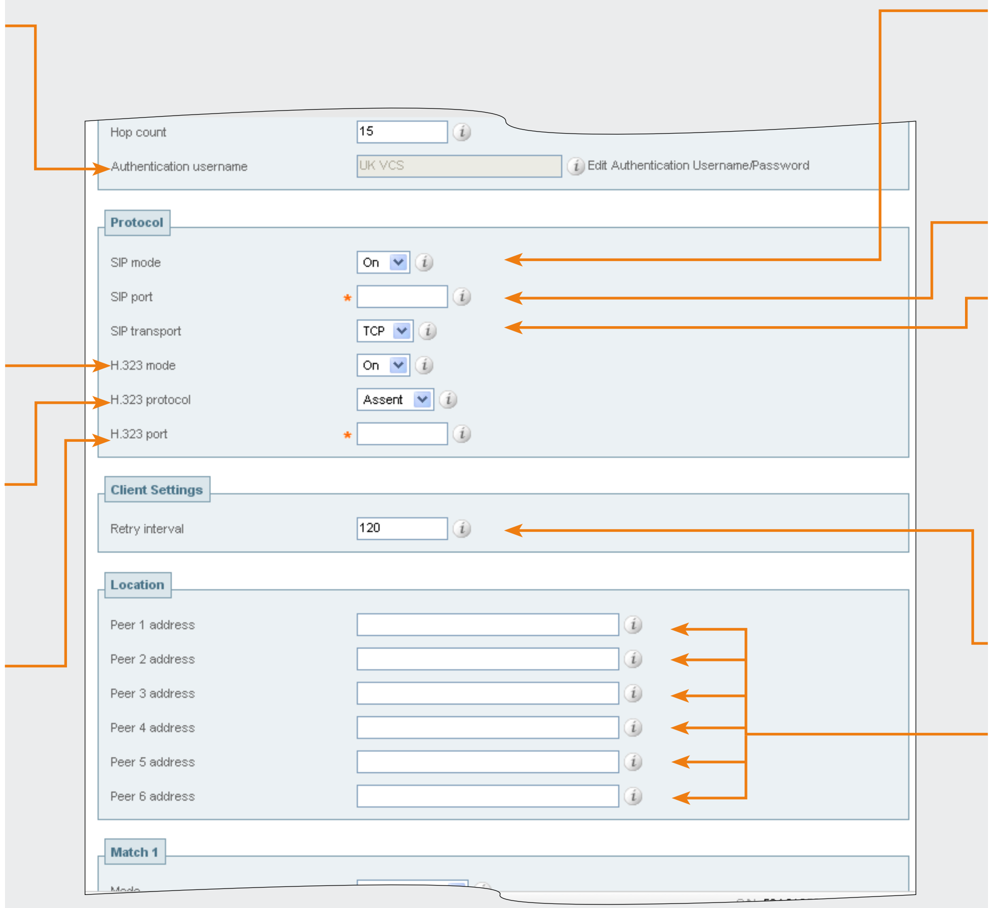
Determines which of the two firewall traversal protocols (Assent or H.460.18) to use for calls to the traversal server. (See Firewall Traversal Protocols for more information.)

H.323 port

Specifies the port on the traversal server to be used for H.323 calls to and from the local VCS.

For firewall traversal to work via H.323, the traversal server must have a traversal server zone configured on it to represent this VCS, using this same port number.

For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see Firewall Traversal.



SIP mode

Determines whether SIP calls will be allowed to and from the traversal server.

SIP port

Specifies the port on the traversal server to be used for SIP calls to and from the VCS.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal server.

For firewall traversal to work via SIP, the traversal server must have a traversal server zone configured on it to represent this VCS, using this same transport type and port number.

Retry interval

Specifies the interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.

Peer 1 to Peer 6 address

The IP Address or FQDN of the traversal server.

If the traversal server is a TANDBERG Border Controller, this should include all its Alternates.

If the traversal server is a VCS cluster, this includes all of its Peers. See the section Neighboring the Local VCS to a Cluster for more information.

NTP must also be configured in order for traversal zones to work.

Configuring Traversal Server Zones

There must be an entry in the traversal server's Authentication database for this username. See Authentication for more information.

Client authentication username

If the traversal client is a VCS, this is its Authentication Username. If the traversal client is a TANDBERG Gatekeeper, this is its System Name.

H.323 mode

Determines whether H.323 calls will be allowed to and from the traversal client.

H.323 protocol

Determines the protocol (Assent or H.460.18) to be used to traverse the firewall/NAT. (See Firewall Traversal Protocols for more information.)

H.323 port

Specifies the port on the local VCS to be used for H.323 calls to and from the traversal client.

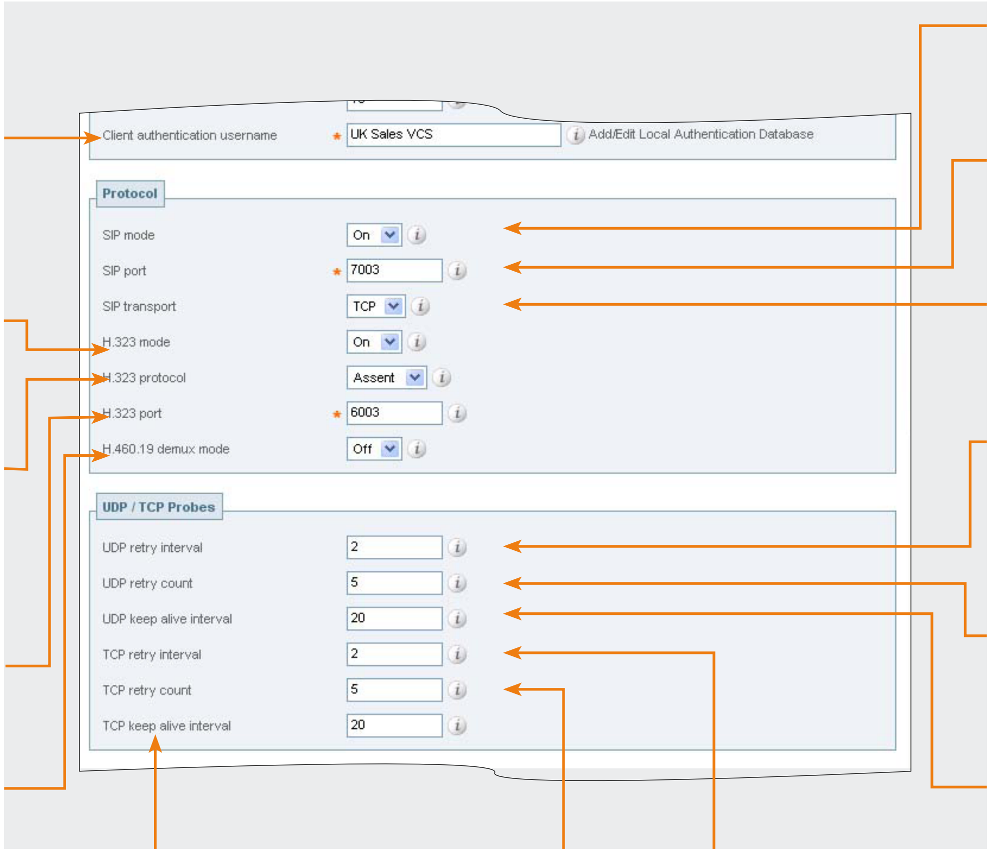
H.460.19 demultiplexing Mode

Determines whether or not the same two ports will be used for media by two or more calls.

On: all calls will use the same two ports.

Off: each call will use a separate pair of ports.

For full details on how traversal client zones and traversal server zones work together to achieve firewall traversal, see Firewall Traversal.



SIP mode

Determines whether SIP calls will be allowed to and from this zone.

SIP port

Specifies the port on the local VCS Expressway to be used for SIP calls to and from the traversal client.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal client.

UDP retry interval

Sets the frequency (in seconds) with which the client will send a UDP probe to the VCS Expressway if a keep alive confirmation has not been received.

UDP retry count

Sets the number of times the client will attempt to send a UDP probe to the VCS Expressway during call setup.

UDP keep alive interval

Sets the interval (in seconds) with which the client will send a UDP probe to the VCS Expressway once a call is established, in order to keep the firewall's NAT bindings open.

TCP keep alive interval

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is in place, in order to maintain the firewall's NAT bindings.

TCP retry count

Sets the number of times the client will attempt to send a TCP probe to the VCS Expressway during call setup.

TCP retry interval

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS if a keep alive confirmation has not been received.

The default UDP and TCP probe retry intervals are suitable for most situations. However, if you experience problems with NAT bindings timing out, they may need to be changed.

Configuring ENUM Zones

DNS suffix

Specifies the domain to be appended to the transformed E.164 number to create an ENUM domain for which this zone is queried.

SIP mode

Determines whether SIP records will be looked up for this zone.

H.323 mode

Determines whether H.323 records will be looked up for this zone.

Full details of how to use and configure ENUM zones is given in ENUM Dialing.



Configuring DNS Zones

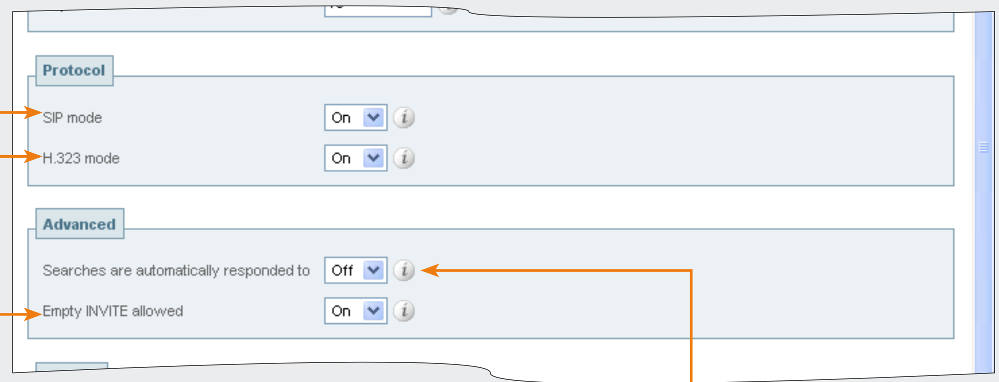
SIP mode

Determines whether SIP calls will be allowed to this zone.

H.323 mode

Determines whether H.323 calls will be allowed to this zone.

Full details of how to use and configure DNS zones is given in URI Dialing.



Empty INVITE allowed

Determines whether the VCS will generate a SIP INVITE messages which has no SDP to send to this zone.

On: SIP INVITEs with no SDP will be generated and sent to this neighbor.

Off: SIP INVITEs with no SDP will be generated but a pre-configured SDP will be inserted before they are sent to this neighbor. The defaults for the SDP are:

Note: In most cases this option should normally be left as the default On. However, some systems such as Microsoft OCS 2007 will not accept invites with no SDP, so for these zones this should be set to Off.

Refer to the relevant TANDBERG VCS Deployment Guide for full details on how to configure these advanced options for specific systems.

Searches are automatically responded to

Determines what happens when the VCS receives a search destined for this zone.

Off: a SIP OPTION message will be sent to the zone.

On: searches will be responded to automatically, without being forwarded to the zone.

Note: In most cases this option should normally be left as the default Off. However, some systems such as Microsoft OCS 2007 will not accept SIP OPTION messages, so for these zones this should be set to On. If you do change this to On, you must also configure pattern matches to ensure that only those searches that actually match endpoints in this zone are responded to.

Refer to the relevant TANDBERG VCS Deployment Guide for full details on how to configure these advanced options for specific systems.

About Clustering

A VCS can be part of a Cluster of up to six VCSs. Each VCS in the Cluster is a Peer of every other VCS in the Cluster.

The purpose of a Cluster is twofold:

- to increase the capacity of your VCS deployment compared with a single VCS
- to provide redundancy in the rare case that a VCS becomes unavailable (for example, due to a network or power outage).

All Peers in a Cluster must use TMS to ensure they are configured identically for subzones, zones, links, pipes, authentication, bandwidth control and call policy. They must also have identical sets of options keys installed. Peers share information with each other about their use of bandwidth, registrations, and FindMe users. This allows the Cluster to act, as one large VCS Local Zone.

The diagram opposite shows four Peers clustered together to form one large Local Zone.

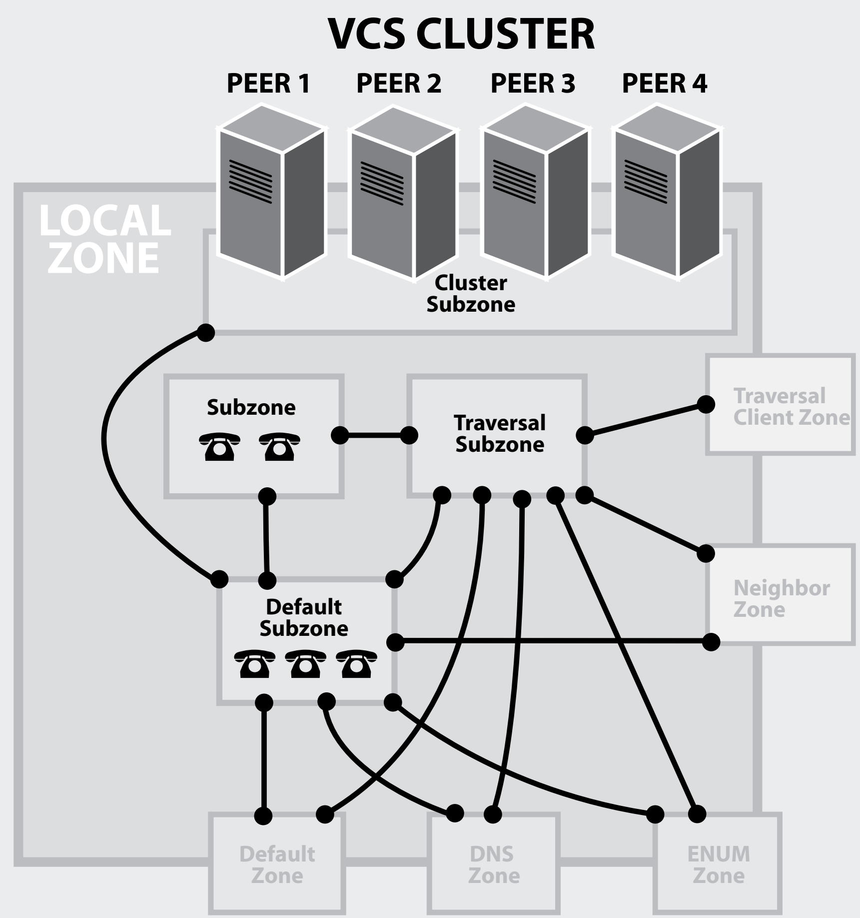
"Alternate" is an H.323 term for a system used to provide redundancy to a Primary gatekeeper, and prior to version X3.0 the VCS supported Alternates. From X3.0 onwards, redundancy (along with other features) is provided by clusters of Peers, which support both H.323 and SIP and work as equals. However, Peers may sometimes be referred to as Alternates.

Cluster Subzone

When two or more VCSs are clustered together, a new subzone is created within the cluster's Local Zone. This is the Cluster Subzone, and any calls between two Peers in the Cluster will pass via this Subzone during call setup. The Cluster Subzone is (like the Traversal Subzone) a virtual Subzone used for call routing only, and endpoints can not register to this subzone. Once a call has been established between two Peers, the Cluster Subzone will no longer appear in the call route and the call will appear as having come from (or being routed to) the Default Subzone.

The two situations in which a call will pass via the Cluster Subzone are:

- Calls between two endpoints registered to different peers in the Cluster.
  For example, Endpoint A is registered in the Default Subzone to Peer 1. Endpoint B is also registered in the Default Subzone, but to Peer 2. When A calls B, the call route is shown on Peer 1 as Default Subzone -> Cluster Subzone, and on Peer 2 as Cluster Subzone -> Default Subzone.
- Calls received from outside the Cluster by one Peer, for an endpoint registered to another Peer.
  For example, we have a single VCS for the Branch Office, which is neighbored to a Cluster of 4 VCSs at the Head Office. A user in the Branch Office calls Endpoint A in the Head Office. Endpoint A is registered in the Default Subzone to Peer 1. The call is received by Peer 2, as it has the lowest resource usage at that moment. Peer 2 then searches for Endpoint A within the Cluster's Local Zone, and finds that it is registered to Peer 1. Peer 2 then forwards the call to Peer 1, which forwards it to Endpoint A. In this case, on Peer 2 the call route will be shown as Branch Office -> Default Subzone -> Cluster Subzone, and on Peer 1 as Cluster Subzone -> Default Subzone.



Configuring Clusters

Prerequisites

Before creating your cluster, ensure that:

- Each VCS to be added to the cluster is configured with a different system name.
- All VCSs to be added to the cluster have different LAN configuration (i.e. a different IPv4 Address and subnet mask, and different IPv6 Address, where enabled).
- All VCSs to be added to the cluster have identical sets of option keys installed.
- Determine which VCS is to be the master and configure it with the settings you wish to apply to the entire cluster.

Enabling H.323

H.323 signaling is used for both endpoint location searching and sharing bandwidth usage information with other Peers in the cluster. This means that H.323 must be enabled on all Peers, even if all endpoints in the cluster are SIP only. To enable H.323, navigate to VCS Configuration > Protocols > H.323 and ensure that H.323 mode is set to On.

TMS

Clusters are created, configured and managed via TANDBERG Management Suite (TMS) version 12.0 and above. To create a cluster using TMS:

1. From Systems > Navigator, select the VCS that will be the Master. This will be the VCS on which all configuration changes are made, and whose configuration is replicated to the other Peers.
2. From the Clustering tab, select Create New Cluster.
3. Enter a Cluster Name and select Create Cluster.
4. You will then have the option to Add Members to the cluster. Select the VCS(s) that are to be Peers in the cluster and click Add.

(For full information, refer to the TMS Administrator Guide.)

TMS will automatically propagate the configuration of the Master to all other Members (Peers) in the cluster. This ensures that configuration across the cluster is kept identical; if it is not, you may experience problems. You must only make configuration changes on the Master. Any changes made on other Peers will not be reflected across the cluster, and will be overwritten the next time the Master's configuration is replicated across the Peers.

We recommend that Peers in a Cluster are deployed on the same LAN as each other so that they can be configured with the same routing information such as local domain names and local domain subnet masks. If Peers are deployed on different LANs, there must be sufficient connectivity between the networks to ensure a low degree of latency between the Peers.

What Configuration is and isn't Replicated?

Most items of configuration are replicated across Peers, with the exceptions listed below.

System Name

The system name is not replicated. It must be different for each Peer in the cluster.

Administration Accounts

The password for the default admin administrator account is not replicated. Each Peer can have a different password.

Any other administration accounts and passwords will be replicated from the Master Peer to all other Peers.

See the Administration Accounts section for further information.

Option keys

Option keys are not replicated. Each Peer must have an identical set of option keys installed, but you must purchase these separately for each Peer in the cluster.

Ethernet speed

The ethernet speed is not replicated. Each Peer may have slightly different requirements for the connection to their ethernet switch.

IP configuration

LAN configuration is not replicated across Peers. Each Peer must have a different IPv4 Address and different IPv6 Address.

The IP Protocol is replicated, because each Peer must support the same protocol(s).

IP Gateway configuration is not replicated. Each Peer can use a different Gateway.

IP routes are not replicated. If these are used, they can be different for each Peer.

DNS Configuration

DNS servers are not replicated across Peers - each Peer can use a different set of DNS servers. However, the DNS domain name is replicated across peers.

Logging

The Event Log and Configuration Log on each Peer will only report activity for that particular VCS. We recommend that you set up a remote syslog server to which the logs of all Peers can be sent. This will allow you to have a global view of activity across all Peers in the cluster.

Clustering, Peers and Alternates

Sharing Registrations Across Peers

When one VCS in a cluster receives a Location Request, it checks its own registration database along with that of each of its Peers before responding. This allows all endpoints in the cluster to be treated as if they were registered with a single VCS.

Peers are periodically queried to ensure that they are still functioning. In order to prevent delays during call setup, any non-functioning Peers will not receive Location Requests.

H.323 Registrations

All the Peers in a Cluster share responsibility for their H.323 endpoint community. When an H.323 endpoint registers with one Peer, it receives a registration response which contains a list of Alternate gatekeepers, populated with the IP addresses of all the other Peers in that Cluster. If the endpoint loses contact with the initial Peer, it will seek to register with one of the Alternates. This may result in your H.323 endpoint community's registrations being spread over all the Peers in the Cluster.

You should change the registration Time to live on all Peers in the Cluster from the default 30 minutes to just a few minutes. This setting determines how often endpoints are required to re-register with their VCS, and changing this to just a few minutes will ensure that if one VCS becomes unavailable, the endpoint will quickly failover to one of its Peers. To change this setting, navigate to VCS Configuration > Protocols > H.323 > Gatekeeper > Time to live.

SIP Registrations

Failover re-registration to an Alternate applies to H.323 re-registrations only. The SIP standard currently has no equivalent. However, if you configure your endpoints with a SIP server address that is an FQDN, and configure this FQDN to resolve to a round-robin DNS record populated with the IP Addresses of all the Peers in the Cluster, then this could allow the endpoint to re-register with another Peer if its connection to the original Peer was lost.

Sharing Bandwidth Across Peers

When clustering has been configured, all Peers share the bandwidth available to the cluster.

Peers must be configured identically for all aspects of bandwidth control including subzones, links and pipes. Peers share their bandwidth usage information with all other Peers in the cluster, so when one Peer is consuming part or all of the bandwidth available within or from a particular subzone, or on a particular pipe, this bandwidth will not be available for other Peers.

For general information on how the VCS manages bandwidth, see the Bandwidth Control section.

Backup and Restore

The Backup and Restore process saves all configuration information for a particular VCS. We recommend that you backup not just the master Peer but all Peers in the cluster. This will ensure that Peer-specific configuration information (see the section What configuration is and isn't replicated?) is saved and can be restored individually for each Peer.

Do not restore a backup made on one Peer to another Peer.

Upgrades and Downgrades

The Clustering feature was introduced to the VCS in software release X3.0.

Upgrading to X3.0

If you are upgrading to VCS software version X3.0 from a previous version and wish to implement clustering, you must:

1. Remove any existing Alternate configuration.
1. Upgrade all VCSs to be added to the cluster to VCS software version X3.0.
2. Determine which VCS will be the master VCS and configure it accordingly.
3. Create and configure the cluster via TMS.
4. Add the remaining Peers to the cluster via TMS.

Downgrading from X3.0

If you have clustering configured and subsequently downgrade to a version of VCS software prior to X3.0, the VCS will retain all its existing configuration but will no longer act as a Peer in a cluster - it will essentially become a stand-alone system. This will have the following impact:

- Changes to the master Peer will not be replicated to the VCS, or if the VCS is the master Peer, its changes will not be replicated to any other VCS.
- The VCS's FindMe database will be a copy of that shared across all Peers in the cluster at the point when the VCS was downgraded. The FindMe database will then be accessible to the local VCS only.
- Other VCSs that were Peers to this VCS will now be treated as Alternates. (See the X2.n Administrator Guide for full information on Alternates.)

Clustering, Peers and Alternates

Clustering and FindMe

Overview

Clustering supports the use of FindMe. Each Peer has its own FindMe database containing all FindMe account information for the cluster. When a FindMe account is created or edited on one Peer, that Peer shares the information about the changes to all other Peers in the cluster, which then update their own FindMe databases accordingly.

Note that the replication of FindMe database information is a completely separate process and uses a different mechanism to the replication of configuration information. Changes to FindMe information can be made on any Peer and will be shared with all other Peers, whereas changes to configuration information can only be made to the master Peer and is then replicated to all other Peers via TMS.

Configuration

Enabling the Replication of FindMe Information

If you are using FindMe on your VCS Cluster, you must first run a special series of commands to allow FindMe databases to be replicated between Peers. Contact your TANDBERG representative for further information on how to do this.

Enabling SSH

The replication of FindMe data between Peers is performed using SSH, so this service must be enabled on all Peers.

To enable SSH, navigate to System Configuration > System and ensure that SSH service is set to On.

Clustering and Presence

Clustering supports the use of Presence.

All Peers in the cluster must have identical SIP Domain, Presence Server and Presence User Agent (PUA) configuration.

If Peers in the cluster have the PUA enabled, each Peer will publish information about its own local registrations. This information will be routed to a Presence Server authoritative for the cluster's domain.

If Peers have the Presence Server enabled, the Presence database is replicated across all Peers in the cluster.

When viewing Presence Status on a Peer in a cluster:

- Publishers will show all presentities across the cluster for whom presence information is being published.
- Presentities will show any presentity for whom a subscription request has been received on the local VCS only.
- Subscribers will show each endpoint from whom a subscription request has been received on the local VCS only.

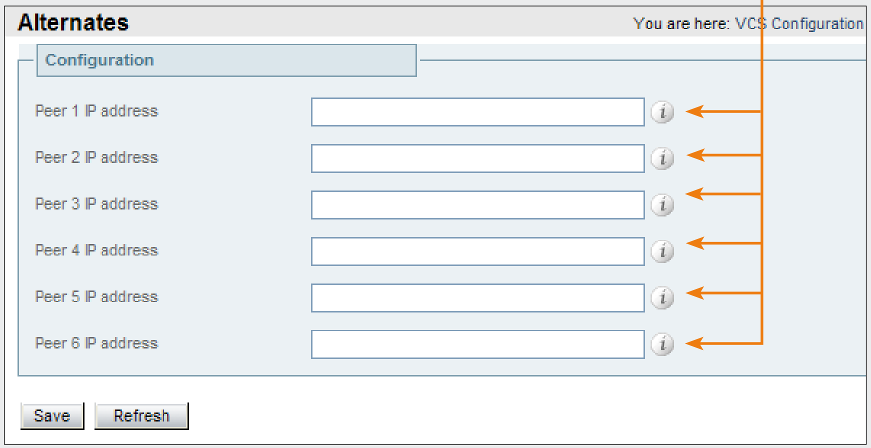
Viewing Peers

The Alternates page lists the IP Addresses of all the Peers in the Cluster to which this VCS belongs, including the IP Address of the VCS to which you are currently logged in.

To view the Alternates page:

- VCS Configuration > Alternates.
  You will be taken to the Alternates page.
- `xConfiguration Alternates`

Do not make any changes directly to this page; it is for information only. Adding and removing Peers from a Cluster must only be done via TMS.



Peer 1...Peer 6 IP address

The IP Addresses of all Peers in the cluster are shown here. This will include the IP Address of the local VCS.

Systems that are configured as Alternates (Peers) must not also be configured as neighbors to each other, and vice versa.

Neighboring the Local VCS to a Cluster

You can neighbor your local VCS (or VCS Cluster) to a remote VCS Cluster; this could be a Neighbor, Traversal Client, or Traversal Server to your local VCS. In this case, when a call is received on your local VCS and is passed via the relevant zone to the remote cluster, it will be routed to whichever Peer in that neighboring cluster has the lowest resource usage. That Peer will then forward the call as appropriate:

- to one of its locally registered endpoints (if the endpoint is registered to that Peer)
- to one of its Peers (if the endpoint is registered to another Peer in that cluster)
- one of its external zones (if the endpoint has been located elsewhere).

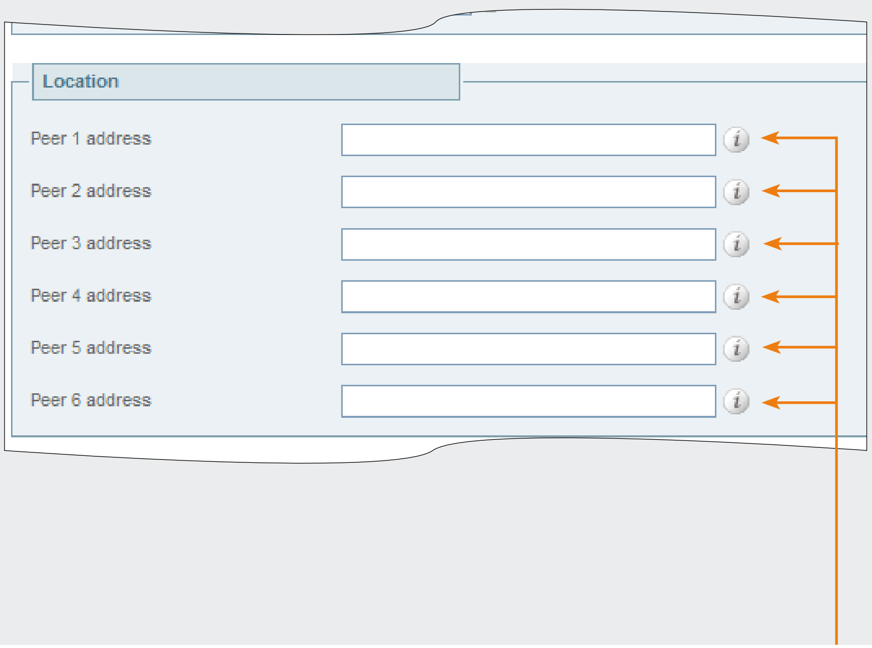
When configuring a connection to a remote Cluster, you should configure the relevant zone with details of all the Peers in the Cluster. Adding this information to the zone will ensure that the call is passed to that Cluster regardless of the status of the individual Peers.

Note that when you are configuring a connection to a remote cluster, you need to enter the IP Address of all Peers only when they are Neighbor or Traversal Client zones. You do not do this for Traversal Server zones, as these are not configured using IP Addresses.

Systems that are configured as Alternates (Peers) must **not** also be configured as neighbors to each other, and vice versa.

The IP Addresses of each Peer in the zone to which you are connecting are configured in the Location section of the Edit Zone page. To access this page:.

- VCS Configuration > Zones.
  You will be taken to the Zones page. From here, click on the name of the zone you wish to edit, or click New to create a new zone.
- `Zones Zone [1..200] Neighbor Peer [1..6] Address`
- `Zones Zone [1..200] TraversalClient Peer [1..6] Address`



Peer 1...Peer 6 address

Enter the IP Address or FQDN of each Peer in the remote cluster.

The order in which the Peers in the remote VCS cluster are listed here does not matter.

Dial Plans

About Dial Plans

As you start deploying more than one VCS, it is useful to neighbor the systems together so that they can query each other about their registered endpoints. Before you start, you should consider how you will structure your dial plan. This will determine the aliases assigned to the endpoints, and the way in which the VCSs are neighbored together. The solution you chose will depend on the complexity of your system. Some possible options are described in the following sections.

Flat Dial Plan

The simplest approach is to assign each endpoint a unique alias and divide the endpoint registrations between the VCSs. Each VCS is then configured with all the other VCS as neighbor zones. When one VCS receives a call for an endpoint which is not registered with it, it will send out a Location Request to all the other neighbor VCSs.

Whilst conceptually simple, this sort of flat dial plan does not scale very well. Adding or moving a VCS requires changing the configuration of every VCS, and one call attempt can result in a large number of location requests. This option is therefore most suitable for a deployment with just one or two VCSs and its Alternates.

Structured Dial Plan

An alternative deployment would use a structured dial plan whereby endpoints are assigned an alias based on the system they are registering with.

If you are using E.164 aliases, each VCS would be assigned an area code. When the VCSs are neighbored together, each neighbor zone is configured with its corresponding area code as a prefix (i.e. a Match Mode of Pattern and a Type of Prefix). That neighbor will now only be queried for calls to numbers which begin with its prefix.

In a URI based dial plan, similar behavior may be obtained by configuring neighbors with a suffix to match the desired domain name.

It may be desirable to have endpoints register with just the subscriber number -- the last part of the E.164 number. In that case, the VCS could be configured to strip prefixes before sending the query to that zone.

A structured dial plan will minimize the number of queries issued when a call is attempted. However, it still requires a fully connected mesh of all VCSs in your deployment. A hierarchical dial plan can simplify this.

Hierarchical Dial Plan

In this type of structure one VCS is nominated as the Directory for the deployment, and all other VCSs are neighbored with it alone. Each VCS is configured with the Directory VCS as a neighbor zone with a Match Mode of Always, and the Directory VCS is configured with each VCS as a neighbor zone with a Match Mode of Pattern and its prefix as the Pattern String.

There is no need to neighbor the VCSs with each other. Adding a new VCS now only requires changing configuration on that system and the Directory VCS.

However, failure of the Directory VCS in this situation could cause significant disruption to communications. Consideration should be given to the use of Clustering for increased resilience.

Call Processing

This section provides information on the pages that appear under the Calls, Transforms and Policy sub-menus of the VCS Configuration menu. These pages allow you to configure the way in which the VCS receives and process calls.

This section includes the following:

- a overview of how the VCS searches for the destination endpoint
- the different types of addresses that can be dialed to initiate a call
- how to apply transforms to the address that was dialed, either before searching on the local VCS or when sending the search request to the Local Zone and external zones
- how to use Call Policy to manage calls
- how to set up your network to handle incoming and outgoing calls made via URI dialing and ENUM dialing
- how to disconnect calls.



Call Processing Diagram

One of the functions of the VCS is to route calls to their appropriate destination, based on the address or alias received from a locally registered endpoint or external zone.

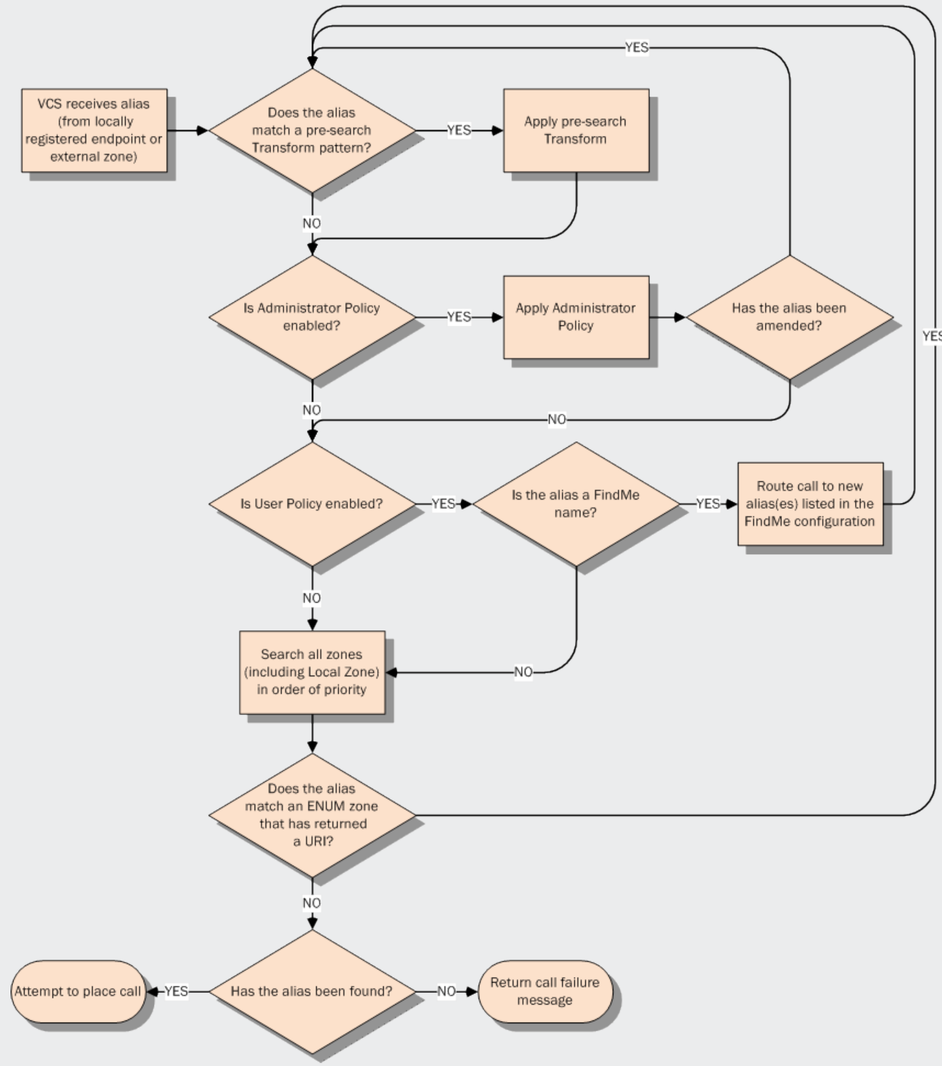
There are a number of steps involved in determining the destination of a call, and some of these steps can involve transforming the alias or redirecting the call to other aliases. It is important to understand the process before setting up your dial plan so you can avoid circular references, where an alias is transformed from its original format to a different format, and then back to the original alias.

The VCS is able to detect circular references. If it does identify one it will terminate that branch of the search and return a "policy loop detected" error message.

Search Process

The process followed by the VCS when attempting to locate a destination endpoint is shown in the diagram opposite.

1. The user enters into their endpoint the alias or address of the destination endpoint. This can be in a number of different formats.
2. The destination address is sent from the caller's endpoint to its local VCS (i.e. the VCS to which it is registered).
3. The VCS applies any pre-search transforms to the alias.
4. The VCS applies any Administrator Policy to the (transformed) alias. If this results in a new alias, the process starts again, with the new alias checked against the pre-search transforms.
5. The VCS applies any User Policy (if FindMe is enabled) to the alias. If the alias is a FindMe name that resolves to one or more new aliases, the process will start again; all the resulting aliases will be checked against pre-search transforms and Administrator Policy.
6. The VCS then searches, in order of priority, all its zones, including the Local Zone (which includes any Peers). If the alias matches an ENUM zone, this may return a URI. If so, the process starts again; the URI is checked against any pre-search transforms, Administrator Policy and User Policy.
7. If the alias is found within the Local Zone or by one of the external zones, the VCS will attempt to place the call to that zone.
8. If the alias is not found, the VCS will respond with a message to say that the call has failed.



Dialing by Address Types

About the Different Address Types

The destination address that is entered via the caller's endpoint can take a number of different formats, and this will affect the specific process that the VCS follows when attempting to locate the destination endpoint. The address types supported by the VCS are:

- IP address e.g. `10.44.10.1` or `3ffe:80ee:3706::10:35`
- H.323 ID e.g. `john.smith` or `john.smith@example.com`
- E.164 alias e.g. `441189876432` or `6432`
- URI e.g. `john.smith@example.com`
- ENUM e.g. `441189876432` or `6432`

Each of these address types may require some configuration of the VCS in order for them to be supported. The following sections describe the configuration required for each address type.

Dialing by H.323 ID or E.164 alias

No special configuration is required in order to place a call using an H.323 ID or E.164 alias. The VCS follows the usual search process, applying any transforms and then searching the Local Zone and external zones for the alias, depending on the match and priority settings of each.

SIP endpoints must register using a URI. We recommend that H.323 endpoints also register with an H.323 ID in the form of a URI to facilitate interworking.

Dialing by IP Address

Dialing by IP address is necessary when the destination endpoint is not registered with any system (e.g. VCS, gatekeeper or Border Controller). If the destination endpoint is registered with one of these systems, then it may still be possible to call it using its IP address but we recommend that one of the other addressing schemes should be used instead as they are more flexible.

In order to make a call by dialing the destination endpoint's IP address, the call must be able to be routed via a VCS that is configured with a Calls to Unknown IP Addresses setting of Direct. This could be the local VCS, or it could be one of its neighbors (in which case the local VCS would route the call to the neighbor, which would then place the call directly to the IP address).

However, if the destination IP address is found in a local subzone (i.e. it is an endpoint registered to the same VCS as the endpoint making the call), then the call will be placed regardless of the Calls to Unknown IP Addresses setting.

Endpoints registered to a VCS Expressway

Calls made by dialing the IP address of an H.323 endpoint registered directly with a VCS Expressway will be forced to route through the VCS Expressway. The call will therefore be subject to any restrictions configured on that system.

If you are calling from an unregistered endpoint, we do not recommend dialing the destination endpoint using its IP address. The presence of a firewall may disrupt the call. Instead place the call to the VCS to which the destination endpoint is registered as described in Calls from an Unregistered Endpoint.

Dialing by H.323 or SIP URI

When a user places a call using URI dialing, they will typically dial name@example.com.

For endpoints that are not locally registered, URI dialing may make use of DNS to locate the destination endpoint. In order to support full URI dialing on the VCS you must configure it with at least one DNS server and at least one DNS zone,

Full instructions on how to configure the VCS to support URI dialing (both outbound and inbound) are given in URI Dialing.

Dialing by ENUM

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias. The E.164 number is converted into a URI by the DNS system, and the rules for URI dialing are then followed to place the call.

The ENUM dialing facility allows you to retain the flexibility of URI dialing whilst having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing via a numeric keypad.

In order to support ENUM dialing on the VCS you must configure it with at least one DNS server and the appropriate ENUM zone(s).

Full instructions on how to configure the VCS to support ENUM dialing (both outbound and inbound) are given in ENUM Dialing.

Hop Counts

About Hop Counts

Each search request is assigned a hop count value by the system that initiates the search. Every time the request is forwarded to another neighbor gatekeeper or proxy, the hop count value is decreased by a value of 1. When the hop count reaches 0, the request will not be forwarded on any further.

For search requests initiated by the local VCS, the hop count assigned to the request is configurable on a zone-by-zone basis. The zone's hop count will apply to all search requests originating from the local VCS that are sent to that zone.

Search requests received from another zone will already have a hop count assigned. When the request is subsequently forwarded on to a neighbor zone, the lower of the two values (i.e. the original hop count or the hop count configured for that zone) will be used.

For H.323, the hop count only applies to search requests. For SIP, the hop count applies to all requests sent to a zone, affecting the Max-Forwards field in the request.

The hop count value can be between 1 and 255. The default is 15.

If your hop counts are set higher than necessary, you may risk introducing loops into your network. In these situations a search request will be sent around the network until the hop count reaches 0, consuming resources unnecessarily.

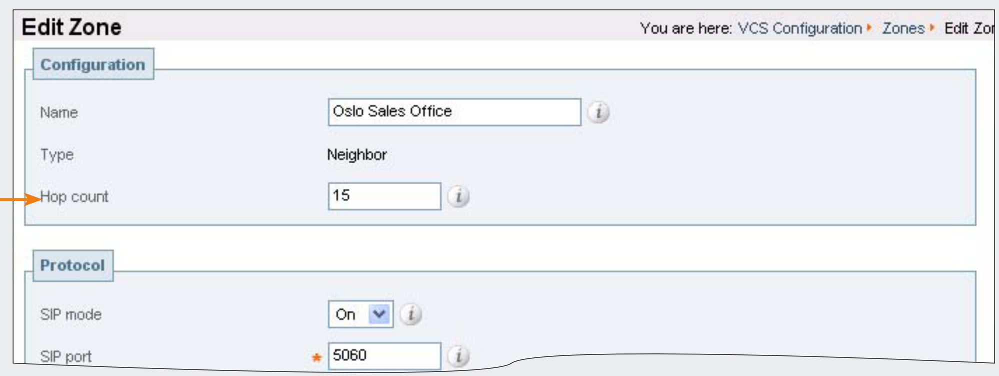
When dialing by URI or ENUM, the hop count used is that for the associated DNS or ENUM zone via which the destination endpoint (or intermediary SIP Proxy or gatekeeper) was found.

Configuring Hop Counts

To configure the hop count for a zone:

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zone page.
  In the Configuration section, in the Hop Count field, enter the hop count value you wish to use for this zone.
- xConfiguration Zones Zone [1..200] HopCount

For full details on other zone options, see Configuring Zones.



Searches and Transforms

Overview of Searches and Transforms

About Searches

One of the VCS's functions is to process incoming requests to search for a particular alias. These search requests are received from

- locally registered endpoints
- neighboring systems, including neighbors, traversal clients and traversal servers
- endpoints on the public internet.

Regardless of the origin of the request, the VCS will search its Local Zone and all external zones for the alias. When creating and configuring zones, you assign at least one match and corresponding priority to each zone, and the zones with the highest priority matches (i.e. those with a priority closest to 1) are searched first. In addition, you can use these pattern matching rules to filter searches to specific zones. For full information about configuring searches, see the Zone Searching and Transforming section.

About Transforms

The VCS allows you to transform the alias in a search request if it matches certain criteria. This transformation can be applied to the alias at two points in the search process:

- as soon as it is received and before it is searched for locally (pre-search Transforms)
- after call policy has been applied and before sending a search request to the Local Zone and external zones.

You can transform the alias by removing or replacing its prefix, suffix, or the entire string, and by the use of regular expressions.

All Peers in a cluster should be configured identically, including any pre-search transforms. A VCS in a cluster will treat search requests from any of its Peers as having come from its own Local Zone, and will not re-apply any pre-search transforms on receipt of the request.

Pre-Search Transforms

About Pre-Search Transforms

The pre-search transform function allows you to modify the alias in an incoming search request. The transformation is applied by the VCS before any searches take place, either locally or to external zones. It applies to all incoming search requests received from locally registered endpoints, Neighbor, Traversal Client and Traversal Server zones, and endpoints on the public internet. It does not apply to requests received from Peers (which are configured identically and therefore will have already applied the same transform).

Each pre-search transform defines a string against which an alias is compared, and the changes to make to the alias if it matches that string.

Once the alias has been transformed, it remains changed. and all further call processing is applied to the new alias.

Pre-search transforms are not applied to GRQ or RRQ messages received from endpoints registering with the VCS; endpoints will be registered with the alias(es) as presented in these messages.

Pre-search transforms will be applied prior to any possible CPL modification and Zone transforms.

Pre-Search Transform Process

Up to 100 pre-search transforms can be configured. Each transform must have a unique priority number between 1 and 65534.

Every incoming alias is compared with each transform in order of priority, starting with that closest to 1. If and when a match is made, the transform is applied to the alias and no further pre-search checks and transformations of the new alias will take place. The new alias is then used for the remainder of the search process.

Further transforms of the alias may take place during the remainder of the search process. This may be as a result of Call Policy (Administrator Policy) or FindMe (User Policy). If this is the case, the pre-search transforms are re-applied to the new alias. Refer to the search process diagram for more information.

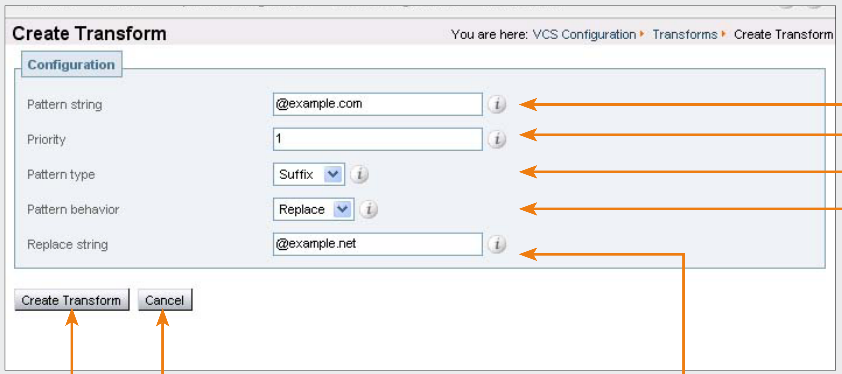
If you add a new pre-search transform that has the same priority as an existing transform, all transforms with a lower priority (i.e. higher numerical value) will have their priority incremented by one, and the new transform will be added with the specified priority. However, if there are not enough "slots" left to move all the priorities down, then you will get an error message.

Pre-Search Transforms

Configuring Pre-Search Transforms

To configure the way in which aliases are transformed before being searched for:

- VCS Configuration > Transforms.
  You will be taken to the Transforms page.
  Click New.
  You will be taken to the Create Transform page.
- xConfiguration Transform [1..100].



Pattern string

Specifies the pattern against which the alias is compared.

Priority

Assigns a priority to this transform. Priority can be from 1 to 65534, with 1 being the highest priority. Transforms are applied in order of priority, and the priority must be unique for each transform.

Pattern type

Determines the way in which the string must match the alias. Options are:

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Pattern behavior

Determines how the matched part of the alias will be modified. Options are:

Strip: the matching prefix or suffix will be removed from the alias.

Replace: the matching part of the alias will be substituted with the text in the Replace String.

Pre-search transforms support the use of Regular Expressions in both the Pattern String and Replace String fields. See the Appendix Regular Expression Reference for more information.

Create Transform

Click here to save the transform and return to the Transforms page.

Cancel

Click here to return to the Transforms page without adding the new transform.

Replace string

(applies only if Pattern Behavior is set to Replace)

Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Zone Searching and Transforming

About Zone Searching

The VCS allows you to filter the search requests sent to each zone, including the Local Zone, and prioritize the order in which these zones are searched. This allows you to reduce the potential number of search requests sent out, and speed up the search process.

The VCS uses the concept of zone "matches" to filter search requests. Each zone has up to five configurable "matches" available to it. Each match is assigned a Mode and Priority (described below). The combination of the two determines if and when that zone will be queried.

Match Mode

The match Mode allows you to specify whether and how requests to the zone will be filtered. You can also use this mode to prevent search requests from ever being sent to the zone.

The Mode options are:

- AlwaysMatch: always query the zone
- PatternMatch: only query the zone if the alias being searched for matches a specified pattern
- Disabled: never query the zone (this mode does not need a corresponding Priority option).

Match Priority

The match Priority allows you to specify when in the search process that zone will be queried. Search requests are sent to all zones with a Priority 1 match first, followed by all zones with Priority 2 matches, and so on.

It is possible for the same priority to be given to more than one match, either in the same zone or in different zones. In this case, all zones with that match priority will be queried at the same time.

About Zone Transforms

The VCS allows you to change the alias being searched for before a search request is sent to the Local Zone or out to a particular zone. This feature uses the PatternMatch mode of the zone search function.

To set up a zone transform, you must:

- configure the zone with a Mode of PatternMatch
- specify the pattern that the alias to be transformed must match
- specify the way in which the alias will be transformed.

All searches that match the specified pattern will then be transformed when sent to the zone, and the zone will be queried using the new alias.

Each zone has up to five configurable matches. This means that you can specify up to five different transforms for each zone. This could be:

- one alias or string transformed five different ways
- five aliases or strings each transformed individually
- a combination of both.

Using Zone Searches and Transforms Together

The zone searching feature and the zone transforms feature both make use of the PatternMatch mode. You can use these two features together or separately.

The remainder of this section:

- describes the zone search and transform process
- explains how to configure zone searches and transforms
- gives some examples of how zone searches and transforms could be used together.

Zone transforms support the use of Regular Expressions in both the Pattern String and Replace String fields. See the Appendix Regular Expression Reference for more information.

Zone Search and Transform Process

Zones searching takes place after call policy has been applied. The zone search and transform process is applied to the Local Zone and all other external zones simultaneously, and is as follows:

1. The VCS looks at all matches for the Local Zone and all external zones to find those with either:
   - a Mode of AlwaysMatch, or
   - a Mode of PatternMatch and a Pattern String that matches the alias being searched for.
2. These matches are listed in order of the Priority that has been assigned to them.
3. If there are any duplicates in the list, the entry with the lower Priority is removed. (This applies to a zone with the same pattern string and the same transform but different priorities.)
4. If there is a zone which has an AlwaysMatch as well as a PatternMatch with no transforms, the PatternMatch is removed from the list.
5. All zones with a Priority 1 match on the list are queried using the same protocol (i.e. SIP or H.323) as the incoming call request. For AlwaysMatch matches, the query will use the original alias; for PatternMatch matches the query will use the alias specified by the transform rules.
6. If the alias is found, the call will be forwarded to that zone. If the alias is found by more than one zone, the call will be forwarded to the zone that responded first.
7. If the alias is not found using the native protocol, the query is repeated (as per steps 5 and 6) using the interworked protocol.
8. If the alias is not found, all zones with a Priority 2 match are queried as per steps 5 to 7.
9. The process is repeated with subsequent Priority levels until either:
   - the alias is found, or
   - all zones with a match that meets the specified criteria have been queried.

Zone Searching and Transforming

Configuring Zone Searches and Transforms

To configure when a zone will be searched and any transforms that will be applied before the search request is sent:

Local Zone

- VCS Configuration > Local Zone > Matches.
  You will be taken to the Local Zone Matches page.
- xConfiguration Zones LocalZone Match [1..5]

External Zones

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click on the zone you wish to configure (or New to create and configure a new zone). You will be taken to the Edit Zone page.
  Scroll down until you get to the Match1 section.
- xConfiguration Zones Zone [1..200] Match [1..5]

Default Settings

By default the Local Zone and all other configured zones have a Match 1 configured with a Mode of AlwaysMatch. All remaining matches will be set to Disabled. This means that (unless you make any changes) the zone will be queried for the original alias, with no transforms applied.

The difference between the default settings for each type of zone is the Priority assigned to Match 1. The default priorities are:

- Local Zone: 50
- Neighbor, Traversal Client or Traversal Server zone: 100
- ENUM or DNS zone: 150

This default configuration means that the Local Zone will be searched first for all aliases. If not found locally, all Neighbor, Traversal Client and Traversal Server zones will then be searched, and if they cannot locate the alias the request will be sent to any DNS and ENUM zones.

You can change the default Match 1 Mode and Priority and add additional Matches for all zones, including the Local Zone.



Mode

Determines if and when a query will be sent to this zone. Options are:

AlwaysMatch: the zone will always be queried.

PatternMatch: the zone will only be queried if the alias queried for matches the specified Pattern String.

Disabled: this match is not used. If all 5 matches for a zone are disabled, the zone will never be queried.

Priority

Determines the order in which the zone will be sent a search request. Zones with priority 1 matches are searched first, followed by priority 2, and so on. More than one match can be assigned the same priority; in this case the matching zones will be queried simultaneously.

Pattern string

(Applies only if the Mode is PatternMatch.)

Specifies the pattern against which the alias is compared.

Pattern type

(Applies only if the Mode is PatternMatch.)

Determines the way in which the string must match the alias. Options are:

Exact: the string must match the alias character for character.

Prefix: the string must appear at the beginning of the alias.

Suffix: the string must appear at the end of the alias.

Regex: the string will be treated as a regular expression.

Replace string

(Applies only if the Mode is PatternMatch and Pattern Behavior is Replace.)

Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Pattern behavior

(Applies only if the Mode is PatternMatch.)

Determines if and how the matched part of the alias will be modified. Options are:

Leave: the alias will not be modified.

Strip: the matching prefix or suffix will be removed from the alias.

Replace: the matching part of the alias will be substituted with the text in the Replace String.

Examples

Combining Match Types and Priorities

By using both AlwaysMatch and PatternMatch matches in the same zone, and applying the same or different priorities to each match, you will have a great deal of flexibility in determining if and when the zone will be queried and whether any transforms will be applied. Some example configurations are given here.

The AlwaysMatch mode does not support alias transforms. Should you wish to always query a zone using a different alias to that received, you will need to use a mode of PatternMatch in combination with a regular expression.

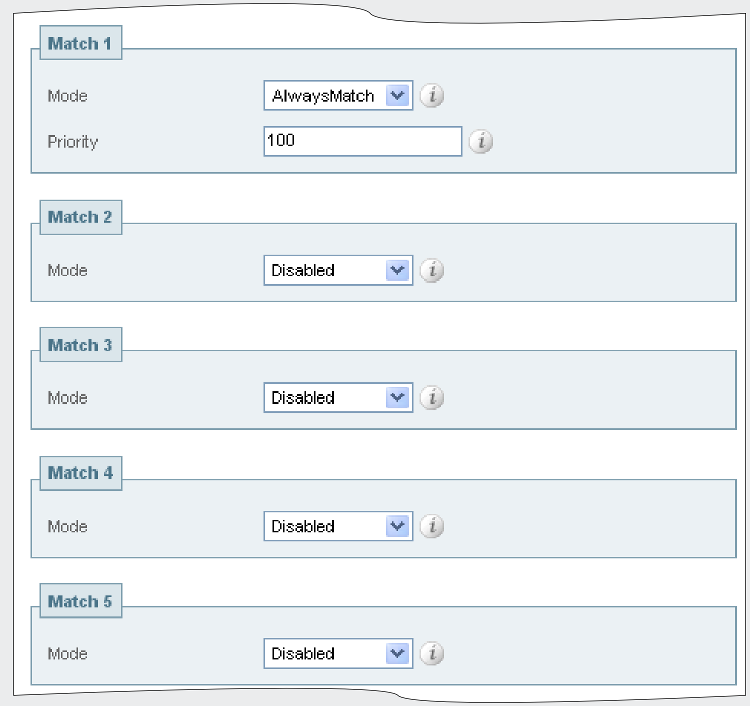
Never Query a Zone

To configure the zone so that it is never sent an alias search request (for example if you only want to receive incoming calls from this zone), set all 5 matches to a Mode of Disabled:



Always Query a Zone, Never Apply Transforms

To configure the zone so that it is always sent search requests using the original alias, set Match 1 to AlwaysMatch with a Priority of 1:



Examples

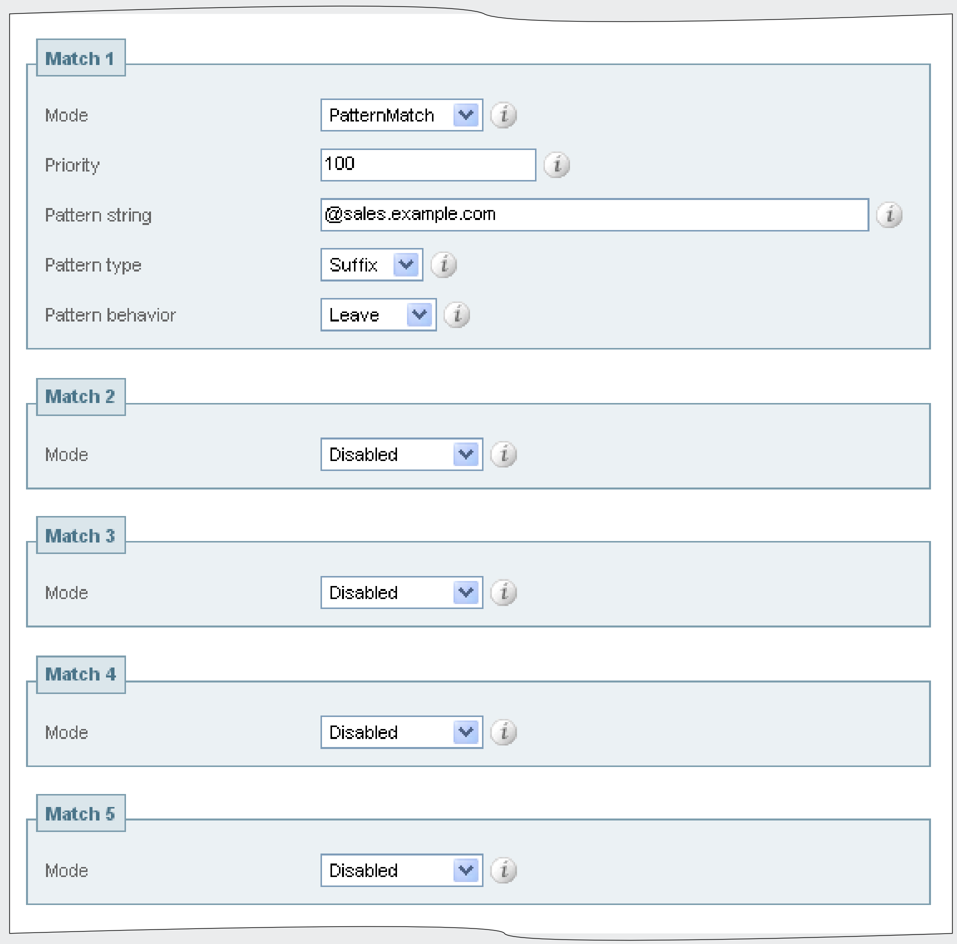
Filter Queries to a Zone Without Transforming

It is possible to filter the search requests sent to a zone so that it is only queried for aliases that match certain criteria.

For example, assume all endpoints in your regional sales office are registered to their local VCS with a suffix of @sales.example.com.

In this situation, it makes sense for your Head Office VCS to query the Sales Office VCS only when it receives a search request for an alias with a suffix of @sales.example.com. Sending any other search requests to this particular VCS would take up resources unnecessarily.

To achieve this, on your Head Office VCS create and configure the zone representing the Sales Office VCS as shown:



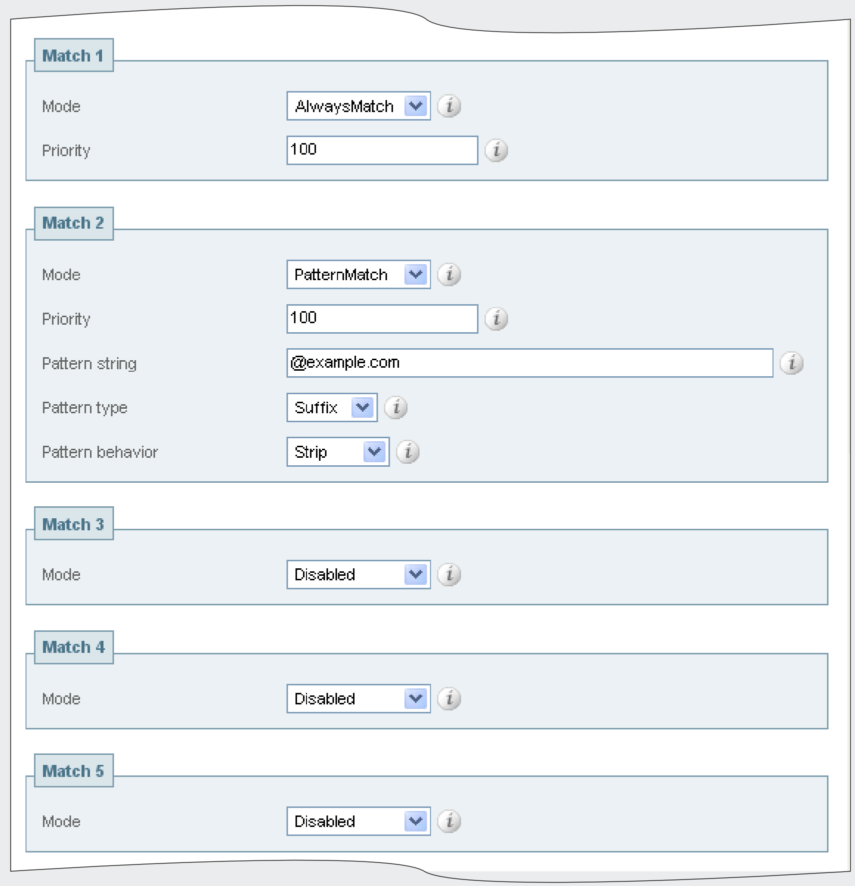
Examples

Query a Zone for Original and Transformed Alias

You may wish to query a zone for the original alias at the same time as you query it for a transformed alias. To do this, configure one match with a mode of AlwaysMatch, and a second match with a mode of PatternMatch along with details of the transform to be applied. Both matches must be given the same Priority level.

For example, you may wish to query a neighbor zone for both a full URI and just the name (i.e. the URI with the domain removed).

To achieve this, on your local VCS configure the zone representing the neighbor VCS as shown:



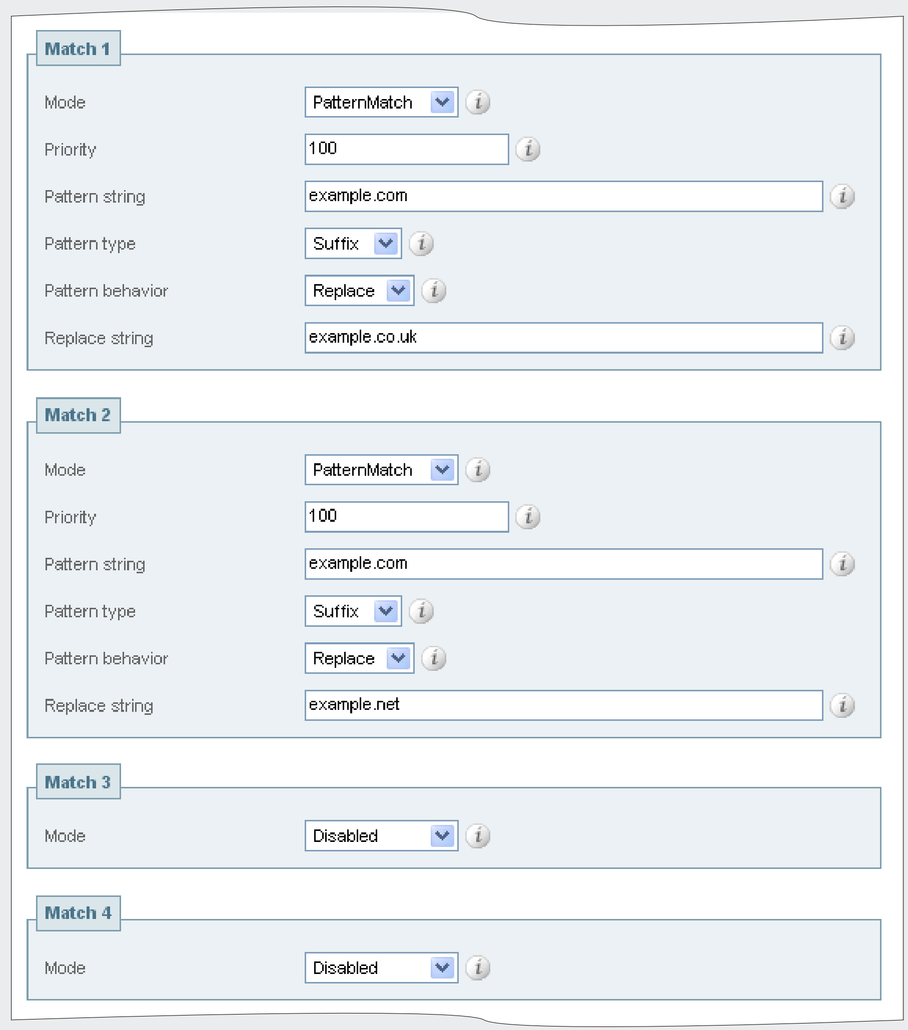
Examples

Query a Zone for Two or More Transformed Aliases

Zones are queried in order of priority of the matches configured within them.

It is possible to configure a single zone with up to five PatternMatch matches, each with the same Priority and with an identical Pattern String to be matched, but each with a different replacement pattern. In this situation, the VCS will query that zone for each of the new aliases simultaneously. (Any duplicate aliases produced by the transforms will be removed prior to the search requests being sent out.)

If any of the new aliases are found by that zone, the call will be forwarded to the zone. It is then up to the controlling system to determine the alias to which the call will be forwarded.



About Call Policy

The VCS allows you to set up a set of rules to control which calls are allowed, which calls are rejected, and which calls are to be redirected to a different destination. These rules are known as Call Policy, or Administrator Policy

If Administrator Policy is enabled and has been configured, each time a call is made the VCS will execute the policy in order to decide, based on the source and destination of the call, whether to

- proxy the call to its original destination
- redirect the call to a different destination or set of destinations
- reject the call.

You can set up an Administrator Policy in either of two ways:

- by configuring basic administrator policy using the web interface. (Note that this will only allow you to Allow or Reject specified calls)
- by uploading a script written in the Call Processing Language (CPL).

Only one of these two methods can be used at any one time to specify Administrator Policy. If a CPL script has been uploaded, this will disable use of the web interface to configure administrator policy. In order to use the web interface, you must delete the CPL script that has been uploaded.

When enabled, Administrator Policy is executed for all calls going through the VCS.

Use Administrator Policy to determine which callers can make or receive calls via the VCS. Use Allow and Deny lists to determine which aliases can or cannot register with the VCS.

Administrator Policy and Authentication

Administrator Policy uses the source and destination of a call to determine the action to be taken. Policy interacts with Authentication when considering the source alias of the call. If your VCS is part of a secure environment, any policy decisions based on the source of the call should only be made when that source can be authenticated. Whether or not the VCS considers an endpoint to be authenticated depends on the Authentication Mode setting of the VCS.

Authentication Mode On

When Authentication Mode is set to On on the VCS, all endpoints and neighbors are required to authenticate with it before calls will be accepted. If a call is received from an unauthenticated source (e.g. neighbor or endpoint) the call's source aliases will be removed from the call request and replaced with an empty field before the Administrator Policy is executed. This is because there is a possibility that the source aliases could be forged and therefore they should not be used for policy decisions in a secure environment. This means that, when Authentication Mode is On and you configure policy based on the source alias, it will only apply to authenticated sources.

The VCS determines whether or not an endpoint is authenticated as follows:

H.323

An H.323 endpoint is considered to be authenticated if either of the following conditions apply:

- it is a locally registered endpoint. (Because Authentication Mode is On, the registration will have been accepted only after the endpoint authenticated successfully with the VCS.)
- it is a remote endpoint that is registered to and authenticated with a Neighbor VCS, and that Neighbor in turn has authenticated with the local VCS.

An H.323 endpoint is considered to be unauthenticated when:

- it is a remote endpoint registered to a neighbor and that neighbor has not authenticated with the VCS. This is regardless of whether or not the endpoint authenticated with the neighbor.

SIP

A SIP endpoint is considered to be authenticated when:

- it falls within one of the domains for which the VCS is authoritative and has successfully responded to an authentication challenge.

A SIP endpoint is considered to be unauthenticated if any of the following conditions apply:

- it does not fall within one of the domains for which the VCS is authoritative, or
- it has failed to successfully respond to an authentication challenge, or
- it has successfully responded to an authentication challenge but its From or Reply-To addresses are not compatible with the alias origin settings.

Authentication Mode Off

When Authentication Mode is set to Off on the VCS, calls will be accepted from any endpoint or neighbor. The assumption is that the source alias is trusted, so authentication is not required.

Administrator Policy

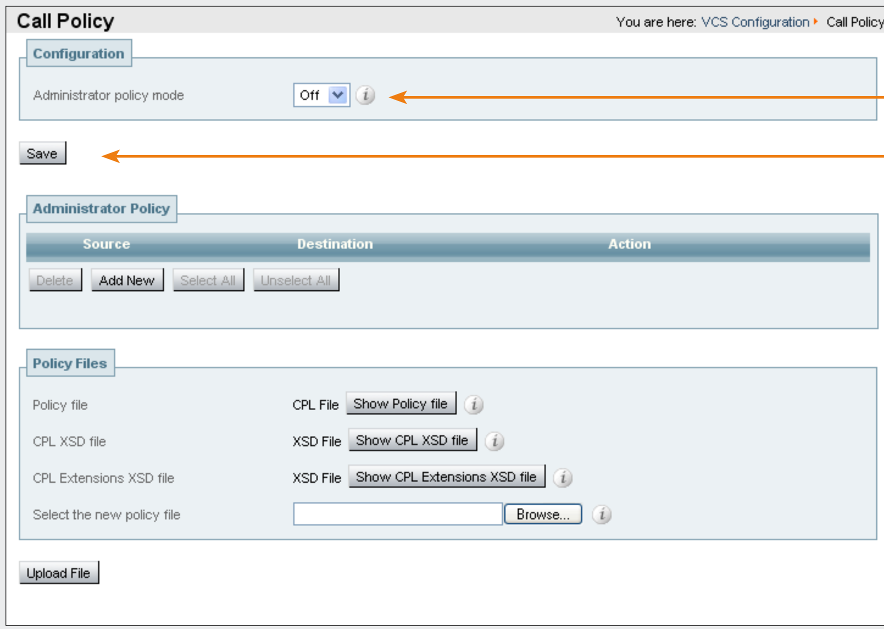
Enabling the use of Administrator Policy

To enable Administrator Policy:

- VCS Configuration > Call Policy.
  You will be taken to the Call Policy page.
- xConfiguration Policy AdministratorPolicy Mode

Once you have enabled the use of Administrator Policy, you must define the policy to be used. This is done either via the web interface or by uploading a CPL script.

If Administrator Policy is on but a policy has not been configured, then a default policy will be applied that allows all calls, regardless of source or destination.



Administrator Policy Mode

On: Administrator Policy is enabled. If a CPL script has been uploaded, this policy will be used. Otherwise, the policy configured via the Administrator Policy section will be used.

Off: Administrator Policy is not in use.

Save

You must click here for any changes to the Administrator Policy Mode to take effect.

Administrator Policy

Configuring Administrator Policy via the Web Interface

To configure Administrator Policy using the web interface:

- VCS Configuration > Policy > Administrator. You will be taken to the Administrator Policy page.

You will not be able to use the web interface to configure Administrator Policy if a CPL file is already in place. If this is the case, you will have the option to Delete Existing file. Doing so will delete the existing Administrator Policy and enable use of the web interface for Administrator Policy configuration.

Administrator Policy

This section shows the web-configured Administrator policy currently in place.

To edit the existing policy, click Add New.

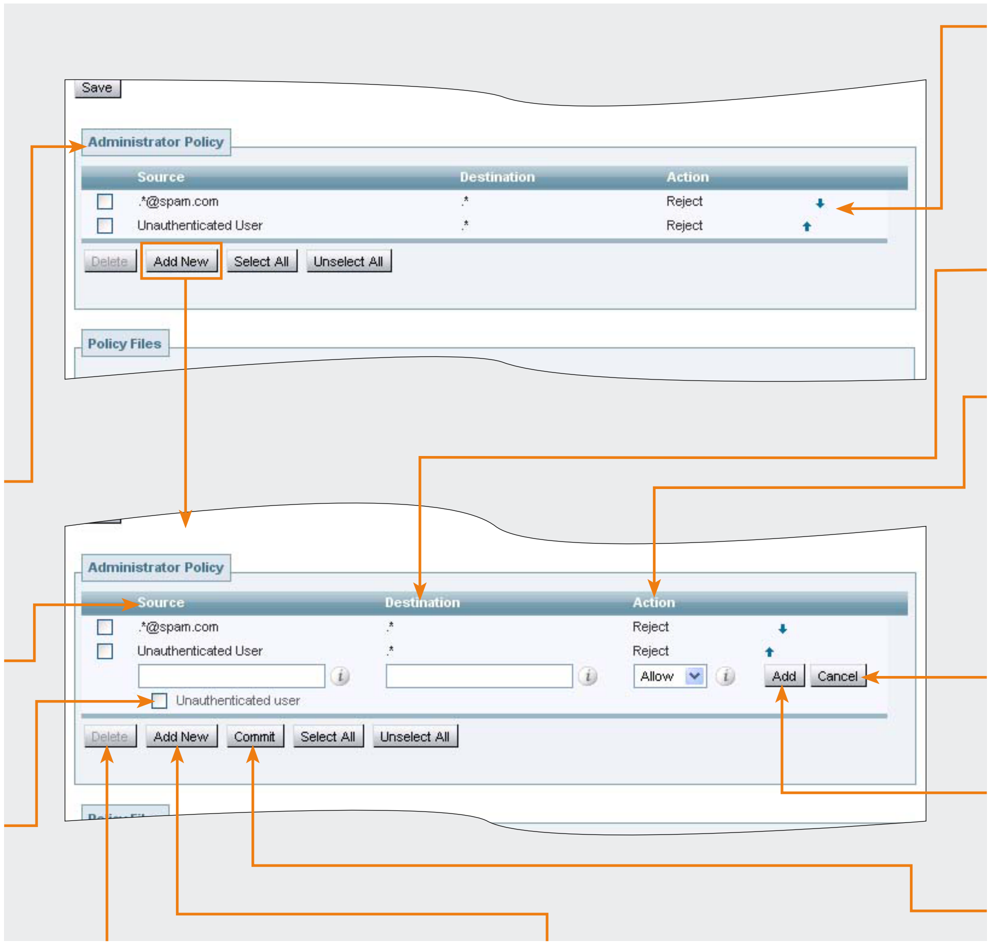
Source

The alias that the calling endpoint used to identify itself when placing the call. This field supports Regular Expressions.

Unauthenticated user

Check this box if you wish the new policy to apply to all incoming calls where the endpoint making the call is *not* either:

- locally registered and authenticated with the VCS, or
- registered and authenticated to a neighbor which in turn has authenticated with the local VCS.



Delete

To remove one or more line items from the list, check the box to the left of the item and then click Delete.

Add New

Click to add the new item to the Policy. A new row with empty fields for you to complete will appear.

↑ and ↓

Each combination of Source and Destination is compared, in the order shown, with the details of the call being made until a match is found. To move a particular item to higher or lower in the list, click on the ↑ and ↓ icons respectively.

Destination

The alias that the endpoint dialed to make the call. This field supports Regular Expressions.

Action

Whether or not the call will be permitted.

Allow: if both the Source and Destination aliases match those listed, call processing will continue.

Reject: if both the Source and Destination aliases match those listed, the call will be rejected.

Cancel

Returns to the Administrator Policy page without adding the new item.

Add

Adds the new item to the Administrator Policy.

Commit

Updates the existing Administrator Policy with the changes you have made.

Administrator Policy

Configuring Administrator Policy via a CPL script

To configure Administrator Policy using a CPL script:

- VCS Configuration > Policy > Administrator. You will be taken to the Administrator Policy page.

Uploading a CPL Script

You can use CPL scripts to configure advanced Administrator Policy. To do this, you must first create and save the CPL script as a text file, after which you upload it to the VCS.

The CPL script cannot be uploaded via the command line interface.

About CPL XSD files

The CPL script must be in a format supported by the VCS. The Administrator Policy page allows you to download the XML schemas which are used to check the script before it is uploaded to the VCS, so you can check in advance that your CPL script is valid.

Select the new policy file

Enter the file name or Browse to the CPL script you wish to upload.

Upload File

Once you have selected the file containing the CPL script, click here to upload it to the VCS.

For information on the CPL syntax and commands that are supported by the VCS, see CPL Reference.



Downloading policy files

Show Policy file

Click here to download the Administrator Policy that is currently in place, as an XML-based CPL script.

- if Administrator Policy has been configured using a CPL script, this will show you the script that was uploaded
- if Administrator Policy has been configured using the web interface, this will show you the CPL version of the policy
- if Administrator Policy is On but a policy has not been configured, this will show you the default CPL script that allows all calls.

You may wish to download the file in order to take a backup copy of the Administrator Policy, or you may want to use the web-configured Administrator Policy as a starting point for a more advanced CPL script.

If you download a web-configured Administrator policy as a CPL script and then upload it back to the VCS without editing it, the VCS will recognise the file and automatically add each rule back into the Administrator Policy section of the web interface.

Show CPL XSD file

Downloads the XML schema used for the CPL script.

Show CPL Extensions XSD file

Downloads the XML schema used for additional CPL elements supported by the VCS.

URI Dialing

Overview

A URI address typically takes the form name@example.com, where name is the alias and example.com is the domain.

URI dialing can make use of DNS to enable endpoints registered with different systems to locate and call each other. With URI dialing, it is possible to find an endpoint by using DNS to locate the domain in the URI address and then query that domain for the alias.

Without URI dialing, you would need to neighbor all the systems to each other in order for one system to be able to locate an endpoint registered to another system. This does not scale well as the number of systems grows. It is also inconvenient for making one-off calls to endpoints registered with previously unknown systems.

H.323 endpoints should register with the VCS using a URI address in order to be reachable using URI dialing. SIP endpoints always register with an AOR in the form of a URI.

There is an exception to the requirement for H.323 endpoints to register with the VCS using a URI address in order to be reachable using URI dialing. This is the case where endpoints register with an alias, and incoming calls are made to alias@domain.com. A local transform is then configured to strip the @domain, and the search is made locally for alias.

If the VCS does not have DNS configured, calls made using URI dialing will still be placed if the destination endpoint is locally registered, or registered to a neighbor system. This is because these endpoints are not located via a DNS query.

URI Resolution Process via DNS

When a VCS is attempting to locate a destination URI address using the DNS system, the general process is as follows:

H323

1. The VCS will send a query (via its DNS server) for a SRV record for the domain in the URI. If available, this SRV record will return information about the authoritative H.323 gatekeeper for that domain (e.g. its FQDN and listening port).
   - If the domain part of the URI address was resolved successfully using an H.323 Location SRV record (i.e. for `_h323ls`) then the FQDN returned is queried via an LRQ for the full URI address.
   - If the domain part of the URI address was resolved using an H.323 Call Signaling SRV record (i.e. for `_h323cs`) or an `A/AAAA` record lookup then the call is routed directly to the IP address returned in that record. An exception to this is where the original dial string has a port specified (e.g. `user@example.com:1720`) in which case the address returned is queried via an LRQ for the full URI address.
   Once its IP address has been discovered, the system will query that gatekeeper for the URI.
2. If a relevant SRV record cannot be located, the system will fall back to looking for an A or AAAA record for the domain in the URI. If such a record is found, the call will be routed to that IP address.

SIP

1. The system will send a NAPTR query for the domain in the URI. If available, the result set of this query will describe a prioritized list of SRV records and transport protocols that should be used to contact that domain.
   If no NAPTR records are present in DNS for this domain name then the VCS will use a default list of _sips._tls.<domain>, _sip._tcp.<domain> and _sip._udp.<domain> for that domain as if they had been returned from DNS.
2. The system will send SRV queries for each result returned from the NAPTR record lookup. A prioritized list of A/AAAA records returned is built. If no SRV records are found then the domain name from the URI is added as the only entry in list of A/AAAA records to lookup.
3. The system will send an A/AAAA record query for each name record returned by the SRV record lookup.

The above steps will result in a tree of IP addresses, port and transport protocols to be used to contact the target domain. The tree is sub-divided by NAPTR record priority and then by SRV record priority. When the tree of locations is used, the searching process will stop on the first location to return a response that indicates that the target destination has been contacted.

If a DNS zone and/or a DNS server have not been configured on the local VCS, calls to non-locally registered endpoints could still be placed if the local VCS is neighbored with another VCS that has been configured for DNS. In this case, any URI dialed calls will go via the neighbor. This configuration is useful if you want all URI dialing to be made via one particular system, e.g. a VCS Expressway.

Enabling URI Dialing

URI dialing is enabled separately for outgoing and incoming calls.

Outgoing Calls

To enable endpoints registered to your VCS to place calls to non-locally registered endpoints directly using URI dialing, you must:

- configure at least one DNS zone, and
- configure at least one DNS Server.

This is described in the section Configuring URI dialing for outgoing calls.

Incoming Calls

To enable endpoints registered to your VCS to receive calls directly from non-locally registered endpoints using URI dialing, you must:

- ensure all endpoints are registered with a URI address
- configure appropriate DNS records, depending on the protocols and transport types you wish to use.

This is described in the section Configuring URI dialing for Incoming calls.

Firewall Traversal Calls

To configure your system so that you can place and receive calls using URI dialing through a firewall, see the section URI Dialing and firewall traversal.

URI Dialing for Outgoing Calls

Process

When a user places a call using URI dialing, they will typically dial an address in the form name@example.com from their endpoint. Below is the process that is followed when a URI address is dialed from an endpoint registered with your VCS:

1. The VCS will check its Local Zone (which includes all Peers in the Cluster to which it may belong) and all its external zones to see if any of them are configured with either:
   - an AlwaysMatch, or
   - a PatternMatch with a pattern that matches the URI address.

   These zones will then be queried in priority order for the URI.
2. If the Local Zone contains a match, the call will be forwarded to the endpoint.
3. If one or more of the external zones that contain a match are neighbor, traversal client or traversal server zone, the zone will be queried for the URI. If the neighbor, traversal client or traversal server supports URI dialing, it may route the call itself.
4. If one or more of the zones that contain a match are DNS zones, this will trigger the VCS to attempt to locate the endpoint through a DNS lookup. It does this by querying the DNS server configured on the VCS for the location of the domain as per the URI resolution process via DNS. If the domain part of the URI address was resolved successfully the request is forwarded to those address(es).

Configuring Matches for DNS Zones

If you wish locally registered endpoints to be able to place URI calls via the VCS, then at a minimum you should configure a DNS zone with a match that has a Mode of AlwaysMatch. This will result in DNS always being queried, but will mean it is queried for all aliases, not just URI addresses.

To filter the queries sent to the DNS server:

- configure a DNS zone with a match that has a Mode of PatternMatch
- use the Pattern string and Pattern type fields to define the aliases that will trigger a DNS query.

For example, a match with a Pattern string of `*@*` and a Pattern type of Regex will mean that DNS is only queried for aliases in the form of typical URI addresses.

To set up further filters, configure the remaining matches in the same DNS zone. You don't need to create new DNS zones unless you want to configure more than the maximum of 5 matches.

You should create separate DNS zones if you want to filter based on the protocol (SIP or H.323) or hop count to be used.

URI Dialing for Outgoing Calls

Adding and Configuring DNS Zones

In order for locally registered endpoints to use URI dialing through the VCS, you must configure at least one DNS zone. To do this:

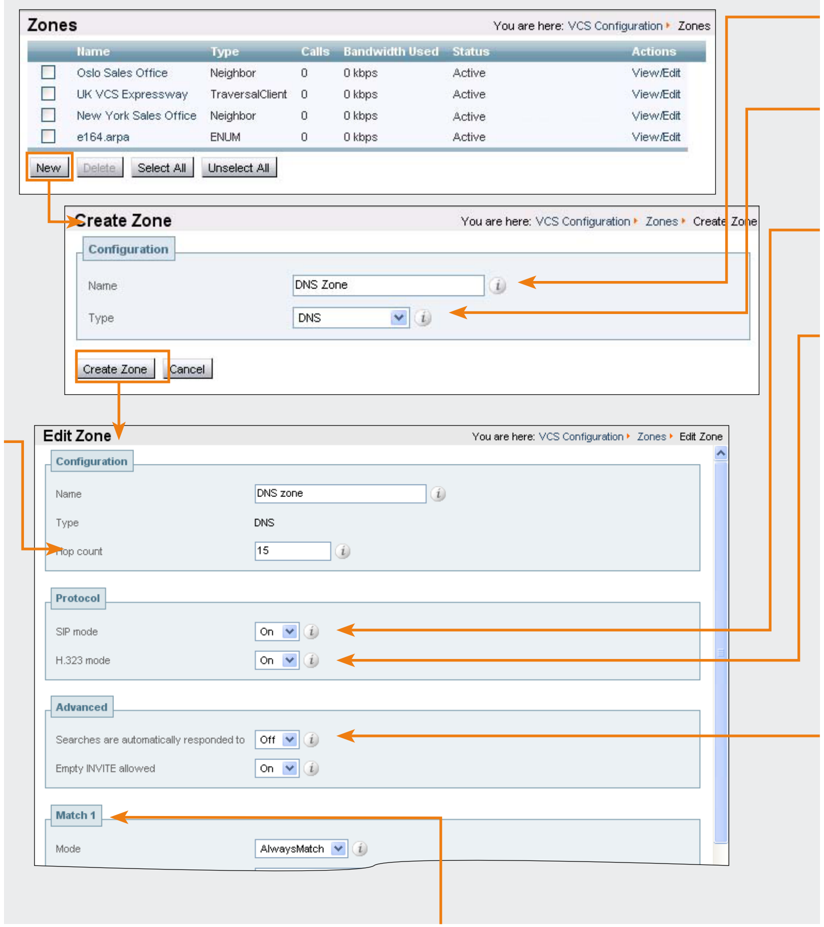
- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click New.
  You will be taken to the Create Zone page.
  Enter a Name for the zone and select a Type of DNS.
  Click Create Zone.
  You will be taken to the Edit Zone page.
- xCommand ZoneAdd
- xConfiguration Zones Zone [1..200]

Hop count

Specifies the hop count to be used when sending an alias search request to this zone. If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

When dialing by URI, the hop count used is that configured for the DNS zone that matches the URI address.

If there is no DNS zone configured that matches the URI address, then the query may be forwarded to a neighbor. In this case, the hop count used will be that configured for the neighbor zone.



Name

Assigns a name to this zone.

Type

For DNS zones, this will be DNS.

SIP mode

Determines whether or not SIP calls will be allowed to this zone.

H.323 mode

Determines whether or not H.323 calls will be allowed to this zone.

Advanced

In most cases the options in the Advanced section should be left at their default values. However, some systems such as Microsoft OCS 2007 may require these options to be changed from the default.

Refer to the relevant TANDBERG VCS Deployment Guide for full details on how to configure these advanced options for specific systems.

Normal zone pattern matching and prioritization rules will apply to DNS zones.

Match1 - Match5

These sections allow you to specify any filtering criteria you wish to apply to this zone.

See Configuring Matches for DNS zones for full information on how the Match options can be used.

URI Dialing for Outgoing Calls

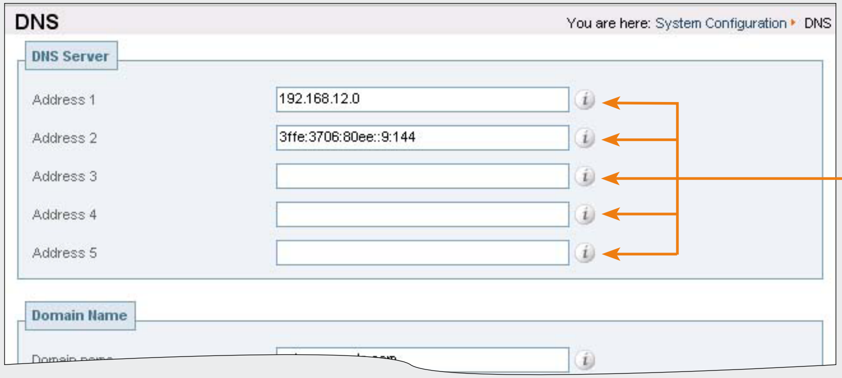
Configuring DNS Servers

To configure the DNS servers to be used by the VCS when querying DNS:

- System Configuration > DNS.
  You will be taken to the DNS page.
- `xConfiguration IP DNS Server`

In order for endpoints registered to the local VCS to make outgoing calls using URI dialing to endpoints that are not registered to the local VCS or one of its neighbors, you must configure at least one DNS server for the VCS to query. For resilience, you can specify up to five DNS servers.

Without DNS, calls made using URI dialing will still be placed if the destination endpoint is locally registered or registered to a neighbor system as locating these URIs does not require the use of DNS.



Address 1 to Address 5

Enter the IP address(es) of up to 5 DNS servers that the VCS will query when attempting to locate a domain.

These fields must use an IP address, not a FQDN.

The DNS server(s) configured here are used as part of both the ENUM dialing and URI dialing processes.

URI Dialing for Incoming Calls

Types of DNS Records Required

The ability of the VCS to receive incoming calls made via URI dialing relies on the presence of DNS records for each domain the VCS is hosting.

These records can be of various types including:

- A records, which provide the IPv4 address of the VCS
- AAAA records, which provide the IPv6 address of the VCS
- Service (SRV) records, which specify the FQDN of the VCS and the port on it to be queried for a particular protocol and transport type.
- NAPTR records, which specify SRV record and transport preferences for a SIP domain.

You should provide an SRV or NAPTR record for each combination of domain hosted and protocol and transport type enabled on the VCS.

Process

When an incoming call has been placed using URI dialing, the VCS will have been located by the calling system via one of the DNS record lookups described above. The VCS will receive the request containing the dialed URI in the form user@example.com. The VCS will then check its local registrations and FindMe names and if any are an exact match, the call will be routed to the appropriate device(s).

SRV Record Format

The format of SRV records is defined by RFC 2782 [3] as:

`_Service._Proto.Name TTL Class SRV Priority Weight Port Target`

For the VCS, these will be as follows:

- `_Service` and `_Proto` will be different for H.323 and SIP, and will depend on the protocol and transport type being used.
- `Name` is the domain in the URI that the VCS is hosting (e.g. example.com)
- `Port` is the port on the VCS that has been configured to listen for that particular service and protocol combination
- `Target` is the FQDN of the VCS.

Configuring H.323 SRV Records

Annex O of H.323 [15] defines the procedures for using DNS to locate gatekeepers and endpoints and for resolving H.323 URL aliases. It also defines parameters for use with the H.323 URL.

The VCS supports two types of SRV record as defined by this Annex. These are Location and Call, with `_Service` set to `_h323ls` and `_h323cs` respectively.

If you wish the VCS to be contactable via H.323 URI dialing, you should provide at least a Location SRV record, as it provides the most flexibility and the simplest configuration.

Location SRV Records

For each domain hosted by the VCS, you should configure a Location SRV record as follows:

- `_Service` is `_h323ls`
- `_Proto` is `_udp`
- `Port` is the port number that has been configured via VCS Configuration > Protocols > H.323 as the Registration UDP port.

Call SRV Records

Call SRV records (and A/AAAA records) are intended primarily for use by endpoints which cannot participate in a location transaction, exchanging LRQ and LCF. The configuration of a Call SRV record should be as follows:

- `_Service` is `_h323cs`
- `_Proto` is `_tcp`
- `Port` is the port number that has been configured via VCS Configuration > Protocols > H.323 as the Call signaling TCP port.

Configuring SIP SRV Records

RFC 3263 [16] describes the DNS procedures used to resolve a SIP URI into the IP address, port, and transport protocol of the next hop to contact.

If you wish the VCS to be contactable via SIP URI dialing, you should configure an SRV record for each SIP transport protocol enabled on the VCS (i.e. UDP, TCP or TLS) as follows:

- Valid combinations of `_Service` and `_Proto` are:
  - `_sips._tcp`
  - `_sip._tcp`
  - `_sip._udp`
- `Port` is the port number that has been configured via VCS Configuration > Protocols > SIP as the port for that particular transport protocol.

URI Dialing

URI Dialing for Incoming Calls

Example DNS Record Configuration

A company with the domain name example.com wants to enable incoming H.323 and SIP calls using URI addresses in the format user@example.com. The VCS hosting the domain has the FQDN vcs.example.com.

Their DNS records would typically be as follows:

- SRV record for _h323ls._udp.example.com returns vcs.example.com
- SRV record for _h323cs._tcp.example.com returns vcs.example.com
- SRV record for _sip._udp.example.com returns vcs.example.com
- SRV record for _sip._tcp.example.com returns vcs.example.com
- SRV record for _sips._tcp.example.com returns vcs.example.com
- A record for vcs.example.com returns the IPv4 address of the VCS
- AAAA record for vcs.example.com returns the IPv6 address of the VCS

How you add the DNS records depends on the type of DNS server you are using. Instructions for setting up two common DNS servers are given in the Appendix DNS Configuration.

In order for locally registered endpoints to be reached using URI dialing, they must register using a full URI. This applies to both SIP and H.323 endpoints. If endpoints do not register using a full URI, they will be discoverable only by the VCS to which they are registered, and any neighbor VCSs.

Several mechanisms could have been used to locate the VCS. You may wish to enable calls placed to user@<VCS_IP_address> to be routed to an existing registration for user@example.com. In this case you would configure a Pre-Search Transform that would strip the IP address of the VCS from the incoming URI and replace it with the domain name of example.com.

URI Dialing and Firewall Traversal

Recommended Configuration

If URI dialing is being used in conjunction with firewall traversal, DNS zones and DNS Servers should be configured on the VCS Expressway and any VCSs on the public network only. VCSs behind the firewall should not have any DNS zones or servers configured. This will ensure that any outgoing URI calls made by endpoints registered with the VCS will be routed through the VCS Expressway.

In addition, the DNS records should be configured with the address of the VCS Expressway as the authoritative gatekeeper/proxy for the enterprise (see the Appendix DNS Configuration). This ensures that incoming calls placed using URI dialing enter the enterprise through the VCS Expressway, allowing successful traversal of the firewall.

ENUM Dialing

Overview

ENUM dialing allows an endpoint to be contacted by a caller dialing an E.164 number - a telephone number - even if that endpoint has registered using a different format of alias.

Using ENUM dialing, when an E.164 number is dialed it is converted into a URI using information stored in DNS. The VCS then attempts to find the endpoint based on the URI that has been returned.

The ENUM dialing facility allows you to retain the flexibility of URI dialing whilst having the simplicity of being called using just a number - particularly important if any of your callers are restricted to dialing via a numeric keypad.

The VCS supports outward ENUM dialing by allowing you to configure ENUM zones on the VCS. When an ENUM zone is queried, this triggers the VCS to transform the E.164 number that was dialed into an ENUM domain which is then queried via DNS.

Note however that ENUM dialing relies on the presence of relevant DNS NAPTR records for the ENUM domain being queried. These are the responsibility of the administrator of that domain.

Process

When a VCS is attempting to dial a destination endpoint using ENUM, the general process is as follows:

1. The user dials the E.164 number from their endpoint.
2. The VCS converts the E.164 number into an ENUM domain as follows:
   a. the digits are reversed and separated by a dot
   b. the name of the domain that is hosting the NAPTR records for that E.164 number is added as a suffix.
3. DNS is then queried for the resulting ENUM domain.
4. If a NAPTR record exists for that ENUM domain, this will advise how the number should be converted into one (or possibly more) H.323/SIP URIs.
5. The VCS begins the search again, this time for the converted URI as per the URI dialing process. Note that this is considered to be a completely new search, and so pre-search transforms and administrator policy will therefore apply.

Enabling ENUM Dialing

ENUM dialing is enabled separately for incoming and outgoing calls.

Outgoing Calls

To allow locally registered endpoints to dial out to other endpoints using ENUM, you must

- configure at least one ENUM zone, and
- configure at least one DNS Server.

This is described in the section Configuring ENUM Dialing for outgoing calls.

Incoming Calls

To enable endpoints in your enterprise to receive incoming calls from other endpoints via ENUM dialing, you must configure a DNS NAPTR record mapping your endpoints' E.164 numbers to their SIP/H.323 URIs. See the section Configuring ENUM dialing for incoming calls for instructions on how to do this.

If an ENUM zone and/or a DNS server have not been configured on the local VCS, calls made using ENUM dialing could still be placed if the local VCS is neighbored with another VCS that has been appropriately configured for ENUM dialing. Any ENUM dialed calls will go via the neighbor. This configuration is useful if you want all ENUM dialing from your enterprise to be configured on one particular system.

ENUM Dialing for Outgoing Calls

Prerequisites

In order for a local endpoint to be able to dial another endpoint using ENUM via your VCS, the following three conditions must be met:

1. There must be a NAPTR record available in DNS that maps the called endpoint's E.164 number to its URI. It is the responsibility of the administrator of the enterprise to which the called endpoint belongs to provide this record, and they will only make it available if they wish the endpoints in their enterprise to be contactable via ENUM dialing.
2. You must configure an ENUM zone on your local VCS. This ENUM zone must have a DNS Suffix that is the same as the domain where the NAPTR record for the called endpoint is held.
3. You must configure your local VCS with the address of at least one DNS server that it can query for the NAPTR record (and if necessary any resulting URI).

Once the ENUM process has returned one or more URIs, a new search will begin for each of these URIs in accordance with the URI dialing process. If the URIs belong to locally registered endpoints, no further configuration is required. However, if one or more of the URIs are not locally registered, you may also need to configure a DNS zone if they are to be located via a DNS lookup.

Process

Below is the process that is followed when an ENUM (E.164) number is dialed from an endpoint registered with your VCS:

1. The user dials the E.164 number from their endpoint.
2. The VCS initiates a search for the E.164 number as dialed. It follows the usual alias search process.
3. After applying any pre-search transforms, the VCS will check all its zones (local and external) and to see if any of them are configured with either:
   - an AlwaysMatch, or
   - a PatternMatch with pattern that matches the E.164 number.

   These zones will then be queried in priority order.
4. If one or more of the zones that contain a match is a neighbor zone, the neighbor will be queried for the E.164 number. If the neighbor supports ENUM dialing, it may route the call itself.
5. If one or more of the zones that contain a match is an ENUM zone, this will trigger the VCS to attempt to locate the endpoint through ENUM. As and when each ENUM zone configured on the VCS is queried, the E.164 number is transformed into an ENUM domain as follows:
   a. the digits are reversed and separated by a dot
   b. the DNS Suffix configured for that ENUM zone is appended.
6. DNS is then queried for the resulting ENUM domain.
7. If the DNS server finds at that ENUM domain a NAPTR record that matches the transformed E.164 number (i.e., after it has been reversed and separated by a dot), it returns the associated URI to the VCS.
8. The VCS then initiates a new search for that URI (maintaining the existing hop count). The VCS starts at the beginning of the search process (i.e. applying any pre-search transforms, then searching local and external zones in priority order). From this point, as it is now searching for a SIP/H.323 URI, the process for URI Dialing is followed.

Example

In this example, we wish to call Fred at Example Corp. Fred's endpoint is actually registered with the URI fred@example.com, but to make it easier to contact him his system administrator has configured a DNS NAPTR record mapping this alias to his E.164 number: +44123456789.

We know that the NAPTR record for example.com uses the DNS domain of e164.arpa.

1. We create an ENUM zone on our local VCS with a DNS suffix of `e164.arpa`.
2. We configure this zone with a pattern match mode of AlwaysMatch, so that ENUM will always be queried regardless of the format of the alias being searched for.
3. We dial `44123456789` from our endpoint.
4. The VCS initiates a search for a registration of 44 118 123 456. Because the ENUM zone we have configured has a match mode of AlwaysMatch, it is queried at the same time as any other zones with a matching priority.
5. Because the zone being queried is an ENUM zone, the VCS is automatically triggered to transform the number into an ENUM domain as follows:
   a. the digits are reversed and separated by a dot: `9.8.7.6.5.4.3.2.1.4.4`
   b. the DNS Suffix configured for this ENUM zone, `e164.arpa`, is appended.

   This results in a transformed domain of `9.8.7.6.5.4.3.2.1.4.4.e164.arpa`.
6. DNS is then queried for that ENUM domain.
7. The DNS server finds the domain and returns the information in the associated NAPTR record. This tells the VCS that the E.164 number we have dialed is mapped to the SIP URI of fred@example.com.
8. The VCS then starts another search, this time for fred@example.com. From this point the process for URI Dialing is followed, and results in the call being forwarded to Fred's endpoint.

ENUM Dialing for Outgoing Calls

Configuring Matches for ENUM Zones

If you wish locally registered endpoints to be able to make ENUM calls via the VCS, then at a minimum you should configure an ENUM zone with:

- a match that has a Mode of AlwaysMatch
- a DNS suffix of e164.arpa (the domain specified by the ENUM standard).

This will result in DNS always being queried for all aliases, not just ENUMs. It will also mean that ENUM dialing will only be successful if the enterprise being dialed uses the e164.arpa domain.

To ensure successful ENUM dialing, you must configure an ENUM zone for each domain that holds NAPTR records for endpoints that callers in your enterprise might wish to dial.

Once these ENUM zones have been created, you can filter the queries that are sent to each as follows:

- configure a match that has a Mode of PatternMatch
- use the Pattern string and Pattern type fields to define the aliases that will trigger an ENUM lookup.

Example

For example, you want to enable ENUM dialing from your network to a remote office in the UK where the endpoints' E.164 numbers start with `44`. You would configure an ENUM zone on your VCS that has a Match configured as follows:

- Mode of PatternMatch
- Pattern string of `44`
- Pattern type of Prefix.

This will result in an ENUM query being sent to that zone only when someone dials a number starting with `44`.

Configuring Transforms for ENUM Zones

You can configure transforms for ENUM zones in the same way as any other zones (see Zone Searching and Transforming for full information).

If there are any transforms configured for an ENUM zone, these will be applied prior to the number being converted to an ENUM domain.

Example

For example, you want to enable ENUM dialing from your network to endpoints at a remote site using a prefix of `8` followed by the last 4 digits of the remote endpoints' E.164 number. You would configure an ENUM zone on your VCS that has a Match configured as follows:

- Mode of PatternMatch
- Pattern string of `8(\d{4})`
- Pattern type of Regex
- Pattern behavior of Replace
- Replace string of `44123123(\1)`

With this configuration, it will be the resulting string (i.e. `44123123xxxx`) that will then be converted into an ENUM domain and queried for via DNS.

To verify that you have configured your outward ENUM dialing correctly, use the `xCommand Locate` command to try and resolve an E.164 alias.

ENUM Dialing for Outgoing Calls

Configuring ENUM Zones

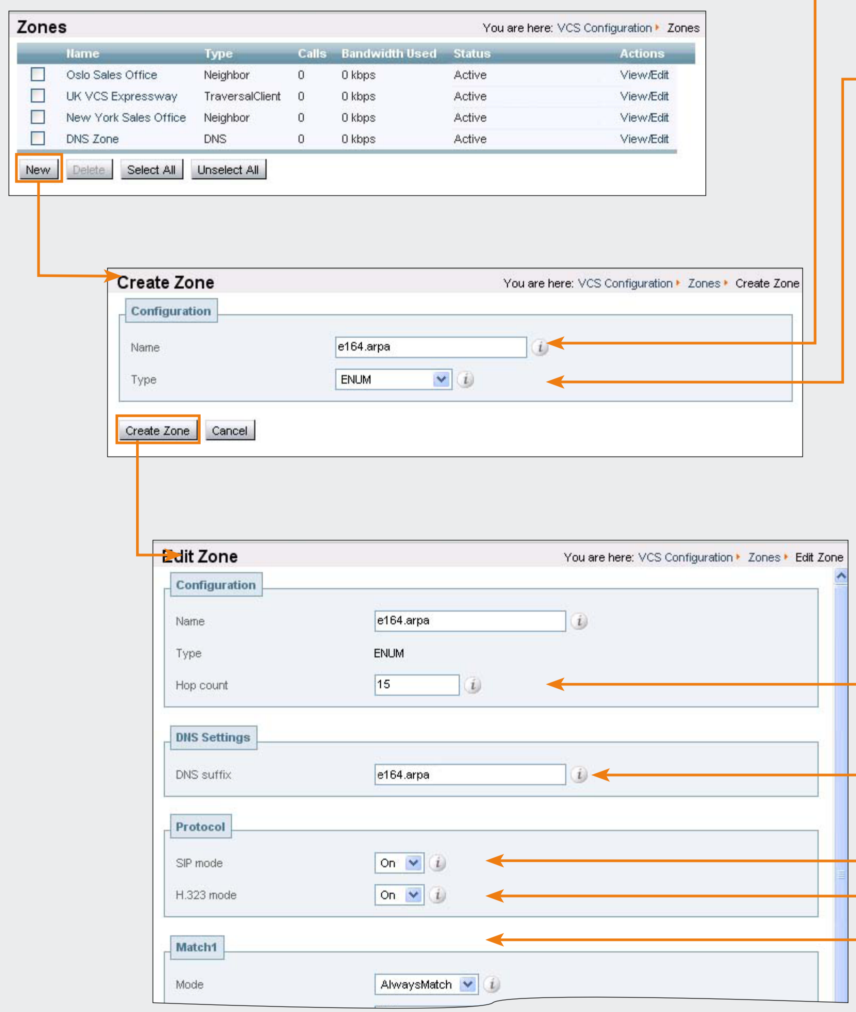
In order for locally registered endpoints to use ENUM dialing, you must configure an ENUM zone for each ENUM service used by remote endpoints. To do this:

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  - Click New.
    You will be taken to the Create Zone page.
  - Enter the zone Name and select a Type of ENUM.
  - Click Create Zone.
    You will be taken to the Edit Zone page.
- xCommand ZoneAdd
- xConfiguration Zones Zone [1..200]

Any number of ENUM zones may be configured on the VCS.

You should configure at least one ENUM zone for each DNS suffix that your endpoints may use.

Normal zone pattern matching and prioritization rules will apply to ENUM zones.



Name
Assigns a name to this zone.

Type
For ENUM zones, this will be ENUM.

Hop count
Specifies the hop count to be used when sending an alias search request to this zone. If the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.

DNS suffix
The DNS zone that is to be queried for a NAPTR record. This suffix is appended to the transformed E.164 number in an attempt to find a matching NAPTR record.

SIP mode
Determines whether or not SIP records will be looked up for this zone.

H.323 mode
Determines whether or not H.323 records will be looked up for this zone.

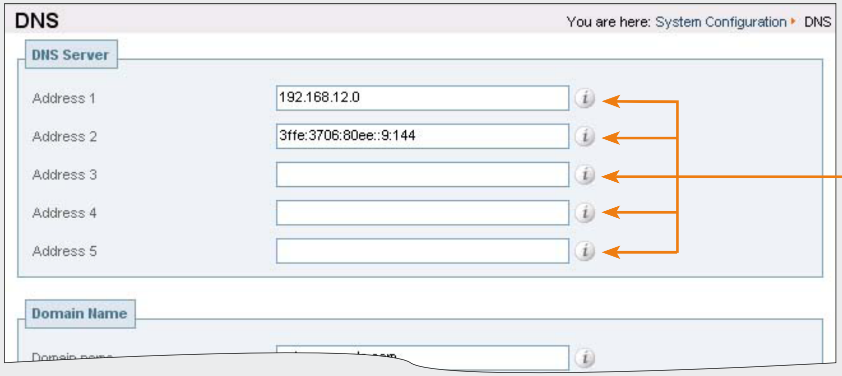
Match1 - Match5
These sections allow you to specify any filtering criteria and/or transforms you wish to apply to this zone. See Configuring Matches for ENUM zones and Configuring Transforms for ENUM zones for full information on how the Match options can be applied.

ENUM Dialing for Outgoing Calls

Configuring DNS Servers

To configure the DNS servers to be used by the VCS when querying DNS:

- System Configuration > DNS.
  You will be taken to the DNS page.
- `xConfiguration IP DNS Server`



Address 1 to Address 5

Enter the IP address(es) of up to 5 DNS servers that the VCS will query when attempting to locate a domain.

In order for endpoints registered to the VCS to make outgoing calls using ENUM dialing, you must configure at least one DNS server for the VCS to query. For resilience, you can specify up to five DNS servers.

The DNS server(s) configured via this page are used as part of both the ENUM dialing and URI dialing processes.

ENUM Dialing for Incoming Calls

Prerequisites

In order for your locally registered endpoints to be reached using ENUM dialing, you must configure a DNS NAPTR record that maps your endpoints' E.164 numbers to their SIP/H.323 URIs. This record must be located at an appropriate DNS domain where it can be found by any systems attempting to reach you via ENUM dialing.

About DNS Domains for ENUM

ENUM relies on the presence of NAPTR records to provide the mapping between E.164 numbers and their SIP/H.323 URIs.

RFC 3761 [8], which is part of a suite of documents that define the ENUM standard, specifies that the domain for ENUM - where the NAPTR records should be located for public ENUM deployments - is e164.arpa. However, use of this domain requires that your E.164 numbers are assigned by an appropriate national regulatory body. Not all countries are yet participating in ENUM, so you may wish to use an alternative domain for your NAPTR records. This domain could reside within your corporate network (for internal use of ENUM) or it could use a public ENUM database such as `http://www.e164.org`.

Configuring DNS NAPTR Records

ENUM relies on the presence of NAPTR records, as defined by RFC 2915 [7]. These are used to obtain an H.323 or SIP URI from an E.164 number.

The record format that the VCS supports is:

- `order flag preference service regex replacement`

where:

- `order` and `preference` determine the order in which NAPTR records will be processed. The record with the lowest `order` is processed first, with those with the lowest `preference` being processed first in the case of matching `order`.
- `flag` determines the interpretation of the other fields in this record. Only the value `u` (indicating that this is a terminal rule) is currently supported, and this is mandatory.
- `service` states whether this record is intended to describe E.164 to URI conversion for H.323 or for SIP. Its value must be either `E2U+h323` or `E2U+SIP`.
- `regex` is a regular expression that describes the conversion from the given E.164 number to an H.323 or SIP URI.
- `replacement` is not currently used by the VCS and should be set to `.` (i.e. the full stop character).

Non-terminal rules in ENUM are not currently supported by the VCS. For more information on these, see section 2.4.1 of RFC 3761 [8].

Example

For example, the record:

- `IN NAPTR 10 100 "u" "E2U+h323" "!^(.*)$!h323:\1@example.com!" .`

would be interpreted as follows:

- `10` is the `order`
- `100` is the `preference`
- `u` is the `flag`
- `E2U+h323` states that this record is for an H.323 URI
- `!^(.*)$!h323:\1@example.com!` describes the conversion:
- `!` is a field separator
- the first field represents the string to be converted. In this example, `^(.*)$` represents the entire E.164 number
- the second field represents the H.323 URI that will be generated. In this example, `h323:\1@example.com` states that the E.164 number will be concatenated with `@example.com`. For example, `1234` will be mapped to `1234@example.com`.
- `.` shows that the `replacement` field has not been used.

Unregistered Endpoints

About Unregistered Endpoints

An unregistered endpoint is any device that is not registered with an H.323 gatekeeper or SIP Registrar (e.g. VCS, gatekeeper or Border Controller). Although most calls are made between endpoints each registered with such a system, it is sometimes necessary to place a call to, or receive a call from, an unregistered endpoint.

Calls from an Unregistered Endpoint

An unregistered endpoint (one that is not registered to any system) can call an endpoint registered with the local VCS.

If there are no firewalls between the unregistered endpoint and the locally registered endpoint, it is possible for the caller to place the call by dialing the locally registered endpoint's IP address. However, we do not recommend that callers are given IP addresses to use as the call may not always be successful (for example if the IP address is private).

Instead, we recommend that callers from unregistered endpoints dial the IP address or the domain name (if configured) of the local VCS, prefixed by the alias they wish to call (for example, john.smith@82.118.9.0). The VCS will then place the call as normal.

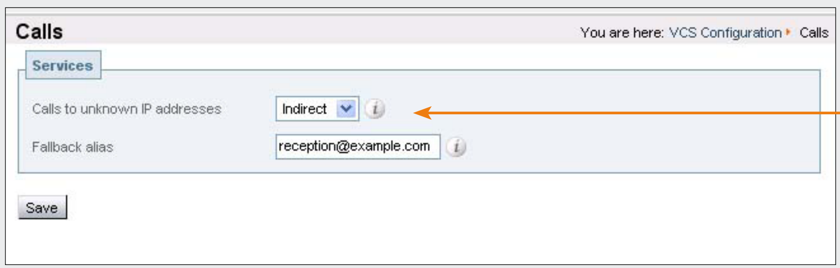
Calls to an Unregistered Endpoint

Overview

Calls can be placed from an endpoint registered to the local VCS to an endpoint that is not registered with any system in two ways:

- using a URI (if the DNS system has been appropriately configured). If URI dialing is used, DNS is queried for a call signaling address and, if found, the call is placed to that address. (See URI Dialing for incoming calls for details of how to configure the Call Signaling SRV Record.)
- dialing its IP address

However, it is sometimes undesirable for a system to be allowed to place a call to an IP address directly. Instead, you may want a neighbor to place the call on behalf of the VCS, or not allow such calls at all. The VCS allows you to configure this behavior.



To configure how the VCS will behave when receiving a call for an IP address that is not registered locally:

- VCS Configuration > Calls
  You will be taken to the Calls page.
- `xConfiguration Call Services`

Calls to Unknown IP Addresses

Determines the way in which the VCS will manage calls to IP addresses which are not registered with it or one of its neighbors.

Direct: A locally registered endpoint will be allowed to make the call to the unknown IP address without the VCS querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.

Indirect: Upon receiving the call the VCS will check to see if the IP address belongs to one of its locally registered H.323 endpoints. If so, it will allow the call. If not, it will query its neighbors for the remote address. If the neighbor's configuration allows it to connect a call to that alias, the VCS will pass the call to that neighbor for completion.

Off: This will not allow any endpoint registered locally to the VCS to call an IP address of any system not also registered locally to that VCS.

Recommended Configuration for Firewall Traversal

When the VCS Expressway is neighbored with an VCS Control for firewall traversal, you should typically set Calls to unknown IP addresses to Indirect on the VCS Control and Direct on the VCS Expressway. When a caller inside the firewall attempts to place a call to an IP address outside the firewall, it will be routed as follows:

1. The call will go from the endpoint to the VCS Control with which it is registered.
2. Since the IP address being called is not registered to that VCS, and its Calls to unknown IP addresses setting is Indirect, the VCS will not place the call directly. Instead, it will query its neighbor VCS Expressway to see if that system is able to place the call on the VCS Control's behalf.
3. The VCS Expressway receives the call and since its Calls to unknown IP addresses setting is Direct, it will make the call directly to the called IP address.

Fallback Alias

Overview

It is possible for the VCS to receive a call that is destined for it but which does not specify an alias. This could be for one of the following reasons:

- the caller has dialed the IP address of the VCS directly
- the caller has dialed the domain name without giving an alias as a prefix
- the caller has dialed the IP address or domain name of the VCS prefixed by the VCS's system name as an alias.

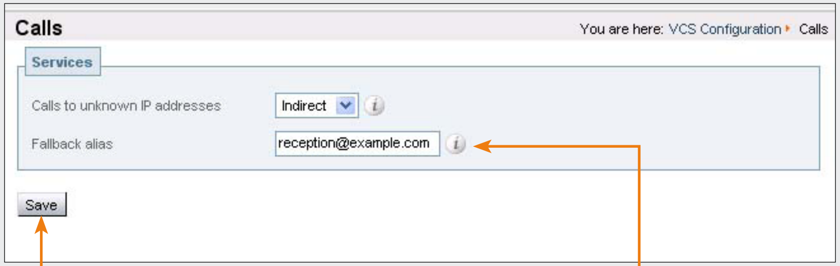
Normally such calls would be disconnected. However, the VCS allows you to specify an alias to which all such calls should be routed. This alias is known as the Fallback Alias.

Some endpoints do not allow users to enter an alias and an IP address to which the call should be placed.

Configuration

To configure the Fallback Alias:

- VCS Configuration > Calls.
  You will be taken to the Calls page.
- `xConfiguration Call Services Fallback Alias`



Save

Click here to save your changes.

Fallback alias

Enter the alias to which you want to forward all calls that do not already specify an alias.

Example Usage

You may wish to configure your Fallback Alias to be that of your receptionist, so that all calls that do not specify an alias will still be answered personally and can then be redirected appropriately.

For example, Example Inc. has the domain of example.com. The endpoint at reception has the alias reception@example.com.

They configure their VCS with a fallback alias of reception@example.com. This means that any calls made directly to example.com (i.e. without being prefixed by an alias), are forwarded to reception@example.com, where the receptionist answers the call and directs it appropriately.

If no fallback alias is configured, calls that do not specify an alias will be disconnected.

Call IDs, Serial Numbers and Tags

Identifying a Particular Call

Each call that passes through the VCS is assigned a Call ID and a Call Serial Number. Calls also have a Call Tag assigned if this does not already exist.

Call ID

The VCS assigns each call currently in progress a different Call ID. The Call ID numbers start at 1 and go up to the maximum number of calls allowed on that system.

Each time a call is made, the VCS will assign that call the lowest available Call ID number. For example, if there is already a call in progress with a Call ID of 1, the next call will be assigned a Call ID of 2. If Call 1 is then disconnected, the third call to be made will be assigned a Call ID of 1.

The Call ID is not therefore a unique identifier: while no two calls in progress at the same time will have the same Call ID, the same Call ID will be assigned to more than one call over time.

Call Serial Number

The VCS assigns a unique Call Serial Number to every call passing through it. No two calls on a VCS will ever have the same Call Serial Number. However, a single call passing between two or more VCSs will be identified by a different Call Serial Number on each system.

Call Tag

Call Tags are used to track calls passing through a number of VCSs. When the VCS receives a call, it checks to see if there is a Call Tag already assigned to it. If so, the VCS will use the existing Call Tag; if not, it will assign a new Call Tag to the call. This Call Tag is then included in the call's details when the call is forwarded on. A single call passing between two or more VCSs will be assigned a different Call Serial Number each time it arrives at a VCS (including one it has already passed through) but can be identified as the same call by use of the Call Tag. This is particularly useful if you are using a remote syslog server to collate events across a number of VCSs in your network.

The Call Tag also helps you identify loops in your network. Loops occur when a query is sent to a neighbor zone and passes through one or more systems before being routed back to the original VCS. In this situation the outgoing and incoming query will have different Call Serial Numbers and may even be for different destination aliases (depending on whether any transforms had been applied). However, the call will still have the same Call Tag.

Call Tags are supported by VCS version X3.0 and above. If a call passes through a system that is not a VCS, or a VCS that is running an earlier version of the software, the Call Tag information will be lost.

Obtaining Call Numbers via the CLI

To control calls using the CLI, you must reference the call using either its call ID or serial number. These can be obtained using the command:

- `xStatus Calls`

This will return details of each call currently in progress in order of their Call ID number. The second line of each entry will list the Call Serial Number, and the third will list the Call Tag.



Call ID

Call serial number

Call tag

Disconnecting Calls

Identifying a Particular Call

Obtaining the Call ID via the Web UI

The Calls page in the web interface lists individual calls based on their Call Serial Number. You can click on a particular call to find out more details about it, including the Call Serial Number and Call Tag. Note that one or more individual calls may have the same Call Tag.

The VCS web UI does not use the Call ID. Calls are identified using their Call Serial number only.

Disconnecting a Call via the Web Interface

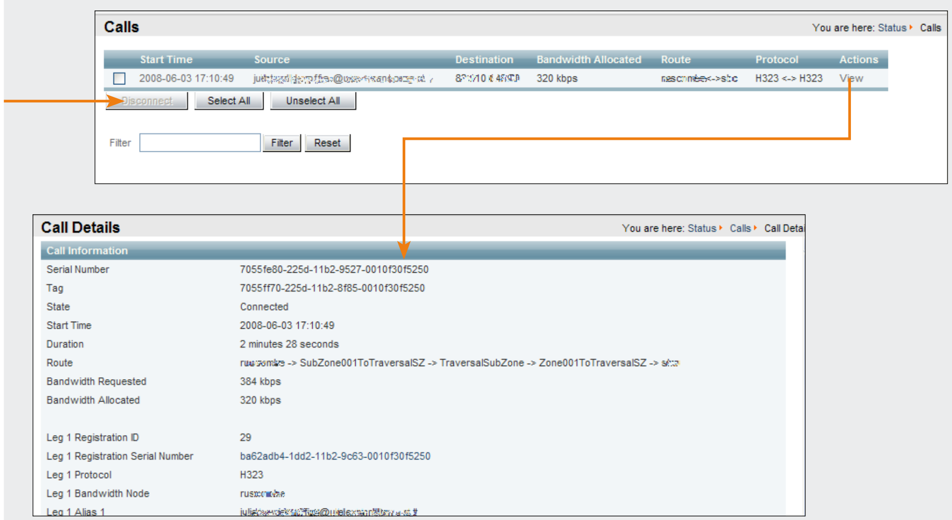
To disconnect one or more existing call via the web interface:

- Status > Calls.
  You will be taken to the Calls page.
  (To check details of a call including the Call Serial Number and Call Tag, click View.)

Disconnect

Check the box next to the call(s) you wish to terminate and select Disconnect.

When disconnecting a call, only the call with that Call Serial Number will be disconnected. Other calls with the same Call Tag but different Call Serial Number may not be affected.



Disconnecting a Call via the CLI

To disconnect an existing call using the CLI, you must first obtain either the call ID number or the call serial number. Then use either one of the following commands as appropriate:

- `xCommand DisconnectCall Call: <ID number>`
- `xCommand DisconnectCall CallSerialNumber: <serial number>`

While it is quicker to use the call ID number to reference the call to be disconnected, there is a risk that in the meantime the call has already been disconnected and the call ID assigned to a new call. For this reason, the VCS also allows you to reference the call using the longer but unique call serial number.

When disconnecting a call, only the call with that Call Serial Number will be disconnected. Other calls with the same Call Tag but different Call Serial Number may not be affected.

Issues when Disconnecting SIP Calls

The call disconnection API works differently for H.323 and SIP calls due to differences in the way the protocols work.

For H.323 calls, and interworked calls, the Disconnect command will actually disconnect the call.

For SIP calls, the Disconnect command will cause the VCS to release all resources used for the call and the call will appear on the system as disconnected. However, SIP calls are peer-to-peer and as a SIP proxy the VCS has no authority over the endpoints. Although releasing the resources may have the side-effect of disconnecting the SIP call, it is also possible that the call signaling, media or both may stay up (depending on the type of call being made). The call will not actually disconnect until the SIP endpoints involved have also cleared their resources.

Endpoints that support RFC 4028 [14] have a call refresh timer which should cause them to clear the resources of any hung SIP calls after a certain period of time. This includes all TANDBERG endpoints.

Bandwidth Control

This section describes the pages that appear under the Local Zone and Bandwidth sub-menus of the VCS Configuration menu in the web interface.

These pages allow you to control the bandwidth that is used for calls within your local zone, as well as calls out to other zones.



Bandwidth Control Overview

Bandwidth Control on the VCS

The TANDBERG VCS allows you to control the amount of bandwidth used by endpoints on your network. This is done by grouping endpoints into subzones, and then applying limits to the bandwidth that can be used:

- within each subzone
- between a subzone and another subzone
- between a subzone and a zone.

Bandwidth limits may be set on a call-by-call basis and/or on a total concurrent usage basis. This flexibility allows you to set appropriate bandwidth controls on individual components of your network.

This section describes the different types of subzones and how to add and configure them, and explains how to use Links and Pipes to apply bandwidth controls between subzones and zones.

Calls will fail if links are not configured correctly. You can check whether a call will succeed, and what bandwidth will be allocated to it, using the command `xCommand CheckBandwidth`.

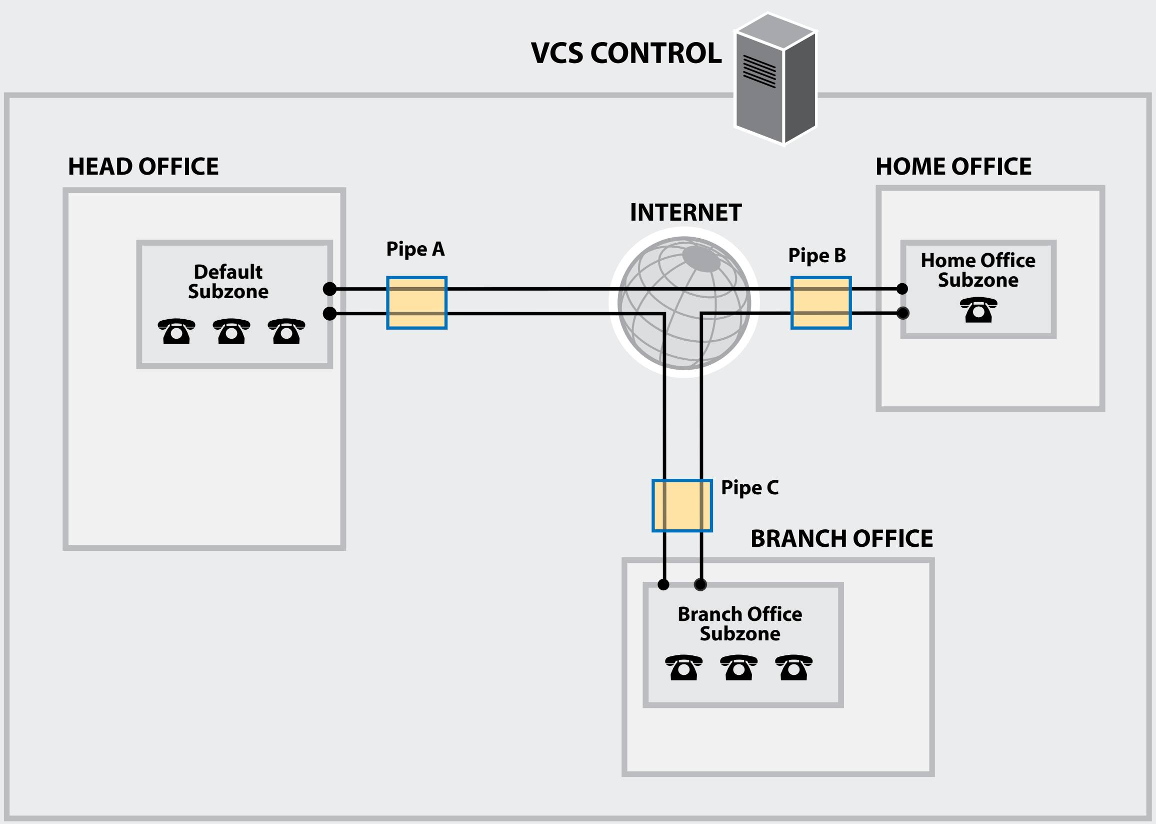
For specific information about how bandwidth is managed across Peers in a cluster, refer to the section Sharing Bandwidth Across Peers.

Example Network Deployment

The diagram below shows a typical network deployment:

- a broadband LAN between the Enterprise and the internet, where high bandwidth calls are acceptable
- a pipe to the internet (Pipe A) with restricted bandwidth
- two satellite offices, Branch and Home, each with their own internet connections and restricted pipes.

In this example we have created new subzone for each pool of endpoints, so that we can apply suitable limitations to the bandwidth used within and between each subzone based on the amount of bandwidth they have available via their internet connections.



Subzones

About Subzones and Bandwidth Control

All endpoints registered with the VCS are part of its Local Zone.

The Local Zone is made up of two or more subzones. The first two subzones are automatically created for you. These are the Default Subzone and the Traversal Subzone. You can create and configure further subzones manually on the basis of endpoints' IP addresses: when an endpoint registers with the VCS its IP address is checked and it is assigned to the appropriate subzone.

The main purpose of all three types of subzones is to enable you to control the bandwidth used by various parts of your network.

About the Default Subzone

When an endpoint registers with the VCS, its IP address is checked and it is assigned to the appropriate subzone. If no subzones have been created, or the endpoint's IP address does not match any of the configured subzones, it will be assigned to the Default Subzone.

The use of a Default Subzone on its own (i.e. without any other manually configured subzones) is suitable only if you have uniform bandwidth available between all your endpoints. However, it is possible for a Local Zone to contain two or more different networks with different bandwidth limitations. In this situation, you should configure separate subzones for each different part of the network.

Specifying the Subzone IP Addresses

A subzone is defined by specifying a range of IP addresses. The VCS allocates endpoints to a subzone based on their IP address. You specify which IP addresses are associated with the subzone by configuring up to 5 subnets for that subzone.

If an endpoint's IP address matches more than one subnet, it will be allocated to the subnet with the narrowest range.

Subzone Links

The VCS is shipped with the Default Subzone and Traversal Subzone (and Default Zone) already created, and with links between the three. You may delete or amend these default links if you need to model restrictions of your network.

If any of these links have been deleted, they may be automatically restored via:

- `xCommand DefaultLinksAdd`

To restore these links via the web interface, you must recreate them manually. See Creating Links for instructions on how to do this.

About the Traversal Subzone

The Traversal Subzone is a conceptual subzone. No endpoints can be registered to the Traversal Subzone; its sole purpose is to allow for the control of bandwidth used by traversal calls.

All traversal calls are deemed to pass through the Traversal Subzone, so by applying bandwidth limitations to the Traversal Subzone you can control how much processing of media the VCS will perform at any one time. These limitations can be applied on a total concurrent usage basis, and/or on a per-call basis.

Traversal Calls

A traversal call is any call passing through the VCS that includes both the signaling (information about the call) and media (voice and video). The only other type of call is a non-traversal call, where the signaling passes through the VCS but the media goes directly between the endpoints.

Traversal calls are always one of the following:

- calls that are traversing a firewall
- SIP to H.323 interworking calls
- IPv4 to IPv6 interworking calls.

Traversal calls use more resource than non-traversal calls, and the numbers of each type of call are licensed separately. The VCS has one license for the maximum number of concurrent traversal calls it can take, and another for the maximum number of concurrent non-traversal calls.

A call is "traversal" or "non-traversal" from the point of view of the VCS through which it is being routed at the time. A call between two endpoints may pass through a series of VCSs. Some of these systems may just take the signaling, in which case the call will be a non-traversal call for that VCS. Other systems in the route may need to take the media as well, and so the call will count as a traversal call on that particular VCS.

Bandwidth Consumption of Traversal Calls

Traversal calls between two endpoints within a single subzone on the VCS must, like all traversal calls, pass through the VCS's Traversal Subzone. This means that such calls will consume an amount of bandwidth from the originating subzone's total concurrent allocation that is equal to twice the bandwidth of the call – once for the call from the subzone to the Traversal Subzone, and again for the call from the Traversal Subzone back to the originating subzone.

In addition, since this call passes through the Traversal Subzone, it will consume an amount of bandwidth from the Traversal Subzone equal to that of the call.

Subzones

Creating a Subzone

To add a new subzone:

- VCS Configuration > Local Zone > Subzones.
  You will be taken to the Subzones page.
  Select New.
  You will be taken to the Create Subzone page.
- xCommand SubZoneAdd

Name

Enter the name you wish to assign to the subzone. You will refer to this name when creating Links.

Subnet 1 address

Enter the IP address of the subnet. In conjunction with the Prefix, this will define the range of IP addresses that will belong to this subzone.

Up to 4 further subnets can be configured once the subzone has been created via the Edit Subzone page.

Prefix length

Enter the number of bits of the Subnet IP Address which must match for an IP address to belong in this subzone.

Address range =

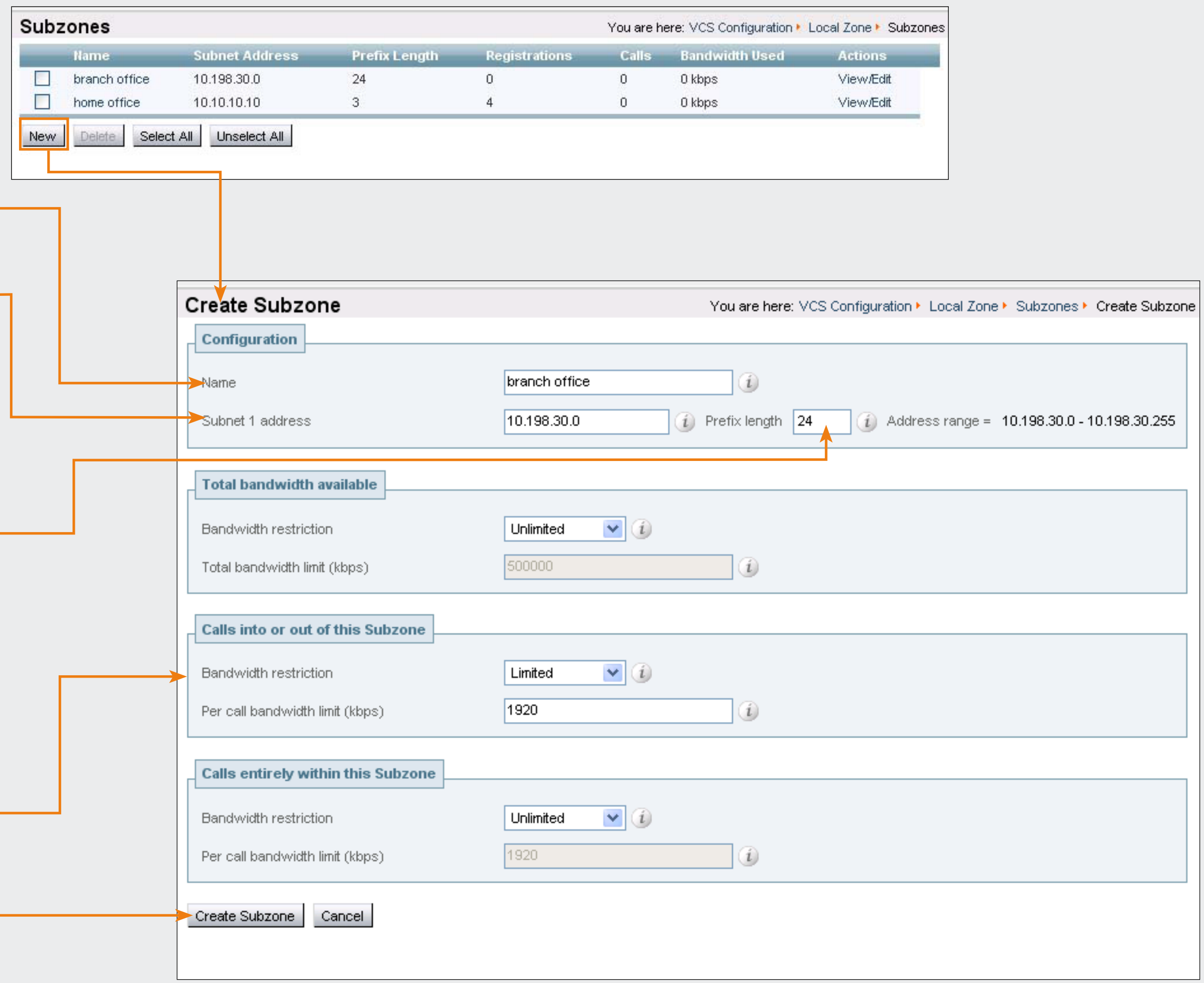
This shows the range of IP addresses that will be allocated to this subzone, based on the combination of the subnet address and prefix length that have been configured.

Bandwidth

See Applying Bandwidth Limitations to Subzones for a description of these fields.

Create Subzone

Click here to create the subzone and return to the subzones page.



Configuring a Subzone

To configure a subzone:

- VCS Configuration > Local Zone > Subzones.
  You will be taken to the Subzones page.
  Click on the subzone you wish to configure.
  You will be taken to the Edit Subzone page.
- xConfiguration Zones LocalZone SubZone

Name

Enter the name you wish to assign to the subzone. You will refer to this name when creating Links and Pipes.

Subnet 1

Enter the subnet IP Address and Prefix, This will define the range of IP addresses that will belong to the first subnet in this subzone.

Address range =

This shows the range of IP addresses that will be allocated to this subzone, based on the combination of the subnet address and prefix length that have been configured.

Subnet 2 - 5

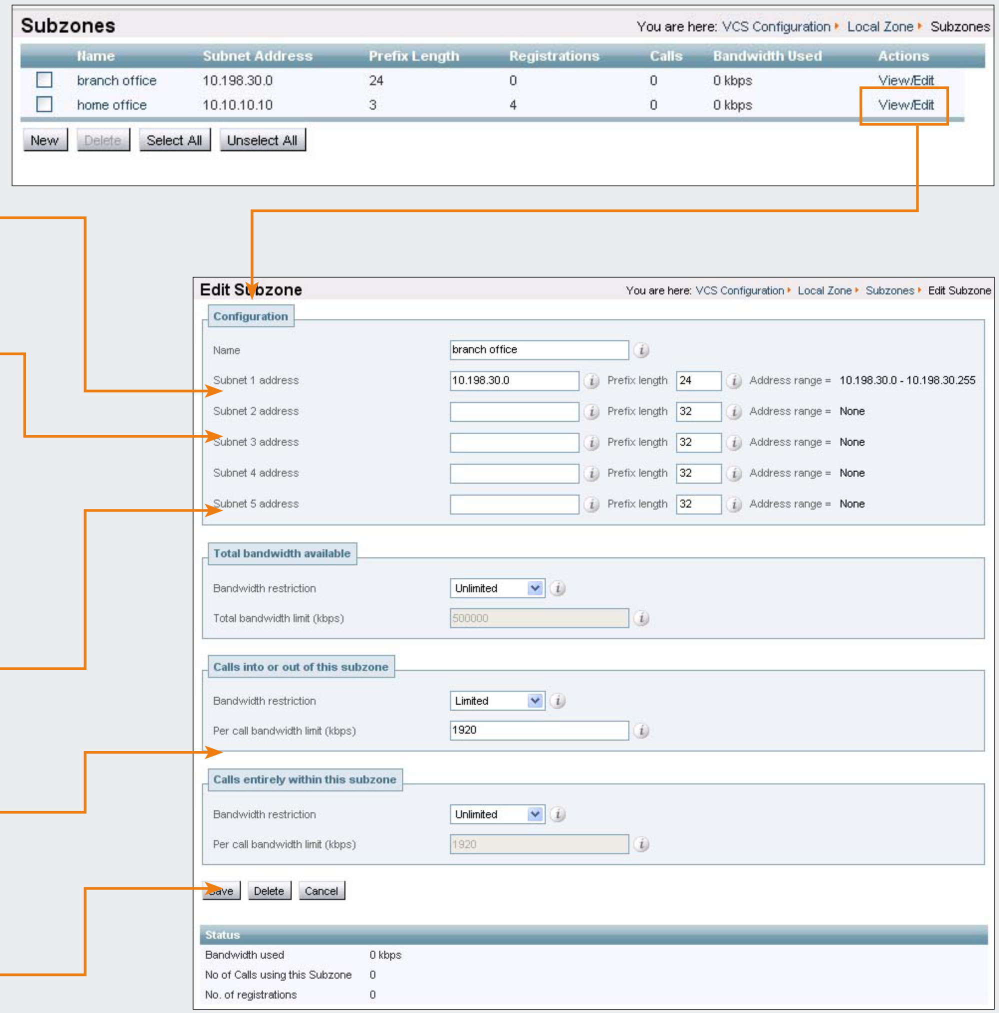
Use these fields to define up to 4 further subnets for this Subzone.

Bandwidth

See Applying Bandwidth Limitations to Subzones for a description of these fields.

Save

Click here to save your changes.



Applying Bandwidth Limitations to Subzones

Types of Limitations

You can apply bandwidth limits to the Default Subzone, Traversal Subzone and all manually configured subzones. The types of limitations you can apply vary depending on the type of subzone, as follows:

Limitation	Description	Can be applied to
Total	Limits the total concurrent bandwidth being used by all endpoints in the subzone at any one time. In the case of the Traversal Subzone, this is the maximum bandwidth available for all concurrent traversal calls.	• Default Subzone • Traversal Subzone • Manually configured subzones
Calls entirely within...	Limits the bandwidth of any individual call between two endpoints within the subzone.	• Default Subzone • Manually configured subzones
Calls into our out of...	Limits the bandwidth of any individual call between an endpoint in the subzone, and an endpoint in another subzone or zone.	• Default Subzone • Manually configured subzones
Calls handled by...	The maximum bandwidth available to any individual traversal call.	• Traversal Subzone

For all these settings, a bandwidth mode of:

- NoBandwidth will mean that no bandwidth is allocated and therefore no calls can be made.
- Limited will mean that limits are applied. You must also enter a value in the corresponding bandwidth (kbps) field.
- Unlimited will mean that no restrictions will be applied to the amount of bandwidth being used.

How Different Bandwidth Limitations are Managed

In situations where there are differing bandwidth limitations applied to the same link, the lower limit will always be the one used when routing the call and taking bandwidth limitations into account.

For example, Subzone A may have a per call inter bandwidth of 128. This means that any calls between Subzone A and any other subzone or zone will be limited to 128kbps. However, Subzone A also has a link configured between it and Subzone B. This link uses a pipe with a limit of 512kbps. In this situation, the lower limit of 128kbps will apply to calls between the two, regardless of the larger capacity of the pipe.

In the reverse situation, where Subzone A has a per call inter bandwidth limit of 512kbps and a link to Subzone B with a pipe of 128, any calls between the two subzones will still be limited to 128kbps.

Use subzone bandwidth limits if you want to configure the bandwidth available between one specific subzone and all other subzones or zones.

Use Pipes if you want to configure the bandwidth available between one specific subzone and another specific subzone or zone.

If your bandwidth configuration is such that multiple types of bandwidth restrictions are placed on a call (for example, if there are both subzone bandwidth limits and pipe limits), the lowest limit will always apply to that call.

A non-traversal call between two endpoints within the same subzone would consume from that subzone the amount of bandwidth of that call. A traversal call between two endpoints within the same subzone must, like all traversal call, pass through the Traversal Subzone. This means that such calls will consume an amount of bandwidth from the originating subzone's total concurrent allocation that is equal to twice the bandwidth of the call – once for the call from the subzone to the Traversal Subzone, and again for the call from the Traversal Subzone back to the originating subzone.

In addition, since this call passes through the Traversal Subzone, it will consume an amount of bandwidth from the Traversal Subzone equal to that of the call.

Links

About Links

Subzones are connected to other subzones and zones via links. For a call to take place, the endpoints involved must each reside in subzones or zones that have a link between them. The link does not need to be direct; the two endpoints may be linked via one or more intermediary subzones.

Links are used to calculate how a call is routed over the network and therefore which zones and subzones are involved and how much bandwidth is available. If multiple routes are possible, your VCS will perform the bandwidth calculations using the one with the fewest links.

Creating a New Link

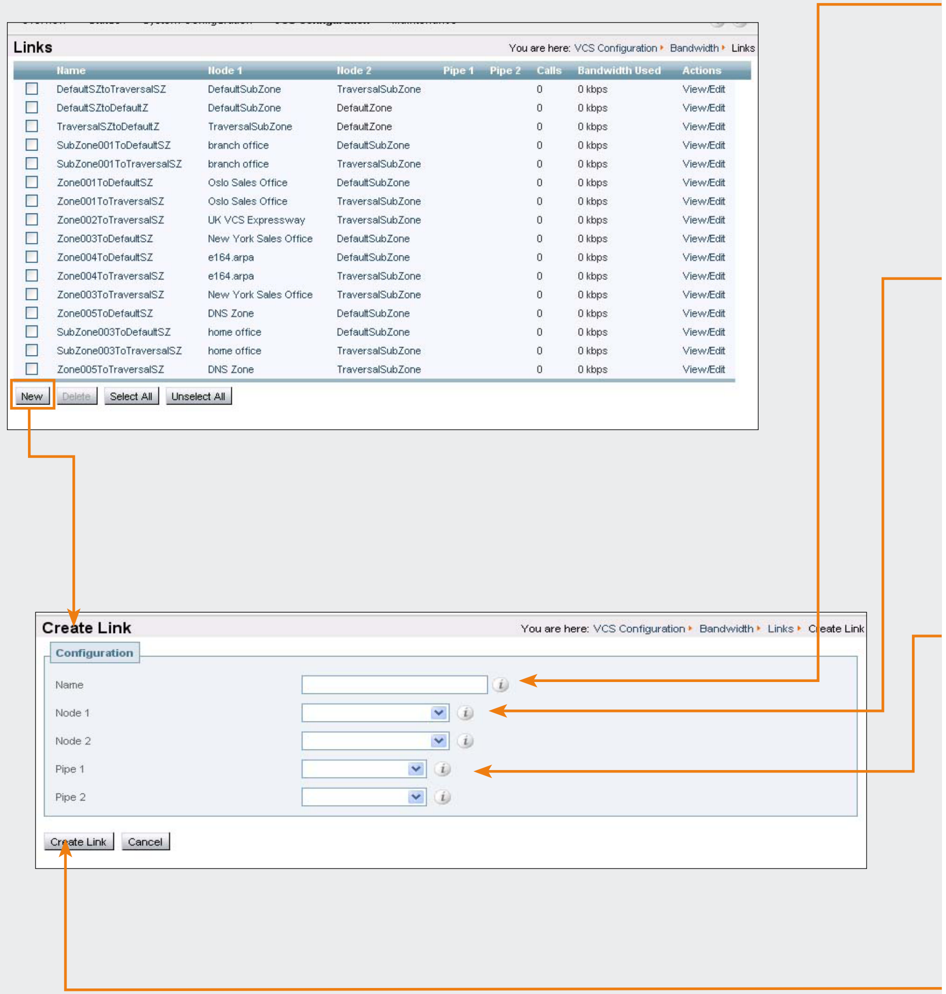
To create a new link:

- VCS Configuration > Bandwidth > Links.
  You will be taken to the Links page.
  Click New.
  You will be taken to the Create Link page.
- xCommand LinkAdd

Default Links

If a subzone has no links configured, then endpoints within the subzone will only be able to call other endpoints within the same subzone. For this reason, when a subzone is created, it is automatically given certain links. See Default Links for more information.

Creating Links



Name

Enter the name you wish to assign to this link.

Node 1, Node 2

Select the names of the two subzones, or the subzone and zone between which you wish to create a link.

Pipe 1, Pipe 2

If you wish to apply bandwidth limitations to this link, select the pipe(s) to be applied.

For more information, see Applying Pipes to Links.

Create Link

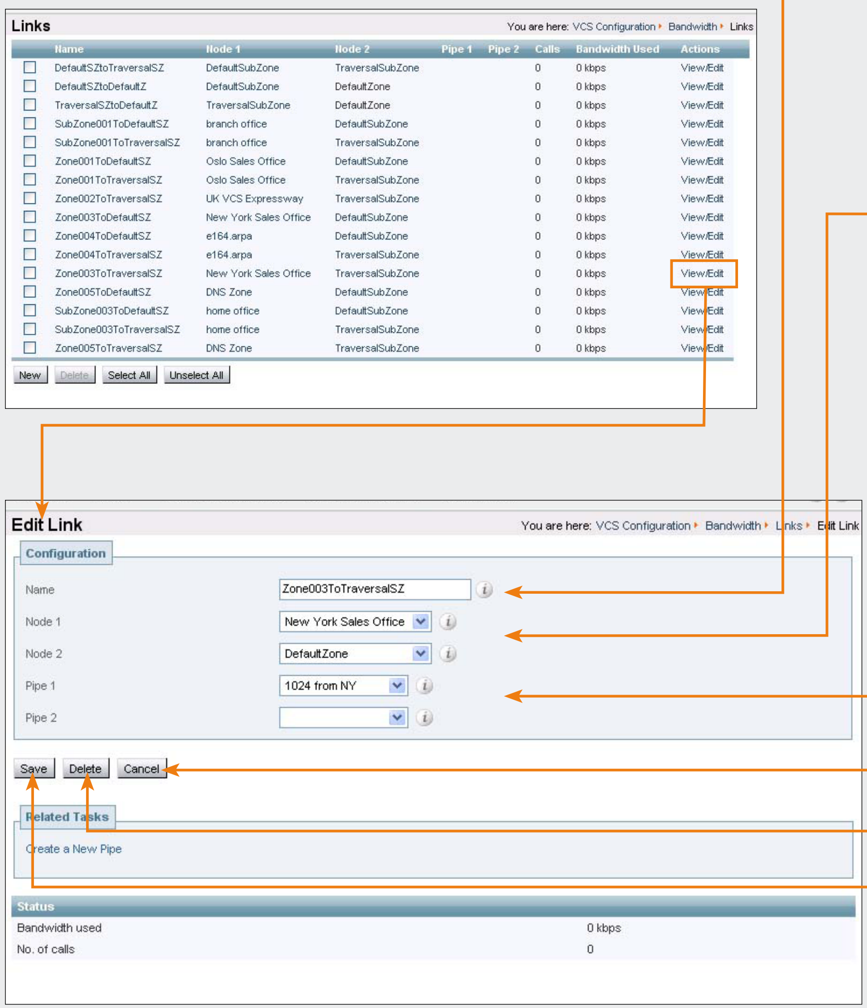
Click here to create the link and return to the Links page.

Links

Editing Links

To edit a link:

- VCS Configuration > Bandwidth > Links.
  You will be taken to the Links page.
  Click View/Edit.
  You will be taken to the Edit Link page.
- xConfiguration Bandwidth Link



Name

Enter the name you wish to assign to this link.

Node 1, Node 2

Select the names of the two subzones, or the subzone and zone between which you wish to create a link.

Pipe 1, Pipe 2

If you wish to apply bandwidth limitations to this link, select the pipe(s) to be applied.

For more information, see Applying Pipes to Links.

Cancel

Click here to return to the Links page without saving your changes.

Delete

Click here to delete the link.

Save

Click here to save your changes.

Default Links

About Default Links

If a subzone has no links configured, then endpoints within the subzone will only be able to call other endpoints within the same subzone. For this reason, the VCS comes shipped with a set of pre-configured links and will also automatically create new links each time you create a new subzone.

Calls will fail if links are not configured correctly. You can check whether a call will succeed, and what bandwidth will be allocated to it, using the command `xCommand CheckBandwidth`.

Pre-Configured Links

The VCS is shipped with the Default Subzone, Traversal Subzone and Default Zone already created, and with default links pre-configured between the three. These links will be named as follows:

- DefaultSZtoTraversalSZ
- DefaultSZtoDefaultZ
- TraversalSZtoDefaultZ

You may rename, delete and amend these default links if you need to model restrictions of your network.

If any of these links have been deleted, they may all be automatically restored via:

- `xCommand DefaultLinksAdd`

To restore these links via the web interface, you must do so manually. See Creating Links for instructions on how to do this.

You can edit any of these default links in the same way you would edit manually configured links. See Editing Links for more information.

Automatically Created Links

Whenever a new subzone or zone is created, links are automatically created as follows:

New zone/subzone type	Default links are created to...
Subzone	Default Subzone and Traversal Subzone
Neighbor zone	Default Subzone and Traversal Subzone
DNS Zone	Default Subzone and Traversal Subzone
ENUM Zone	Default Subzone and Traversal Subzone
Traversal Client Zone	Traversal Subzone
Traversal Server Zone	Traversal Subzone

Along with the pre-configured default links this ensures that, by default, any new subzone or zone has connectivity to all other subzones and zones. You may rename, delete and amend any of these default links.

About Pipes

It is possible to control the amount of bandwidth used on calls between specific subzones and zones. The limits can be applied to the total concurrent bandwidth used at any one time, or to the bandwidth used by any individual call.

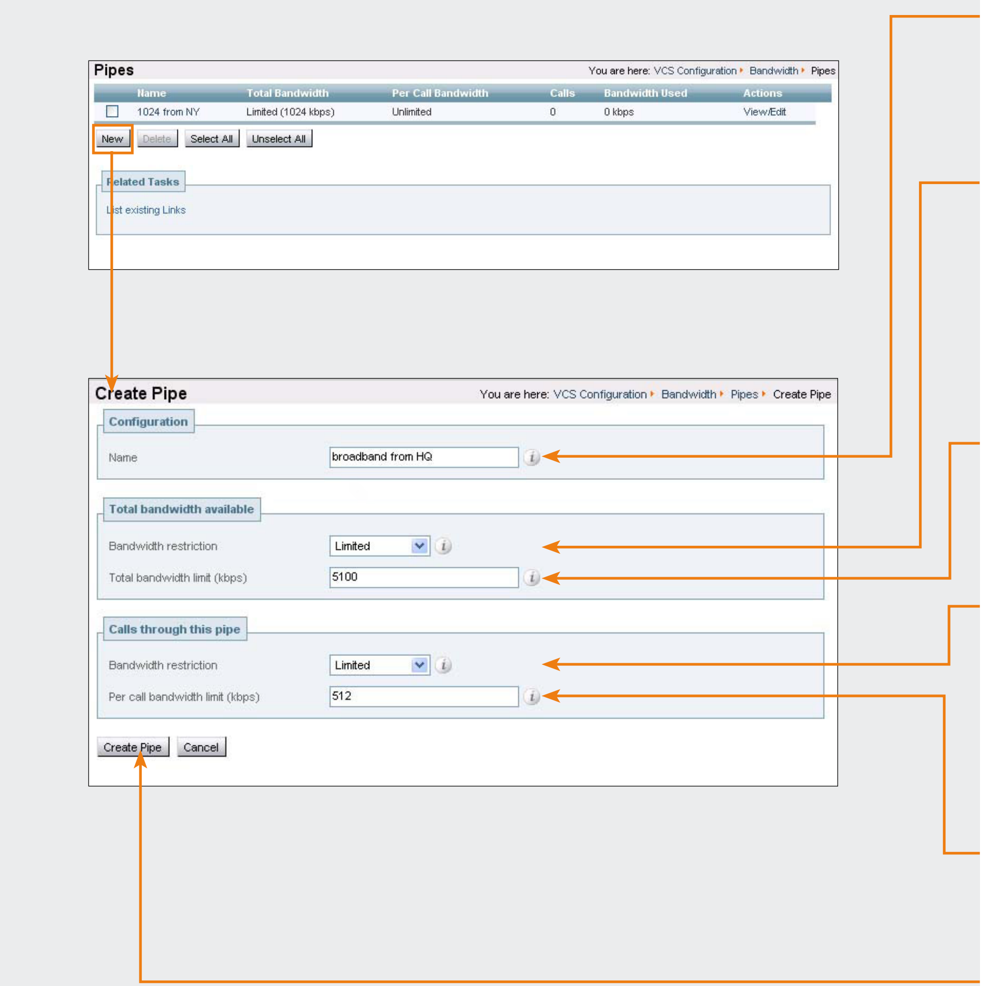
To apply these limits, you create a pipe and configure it with the required bandwidth limitations. Then when configuring links you assign the pipe to one or more links. Calls using the link will then have the pipe's bandwidth limitations applied to them.

See Applying Pipes to Links for more information.

To create a pipe:

- VCS Configuration > Bandwidth > Pipes.
  You will be taken to the Pipes page.
  Select New.
  You will be taken to the Create Pipe page.
- `xCommand PipeAdd`

Creating Pipes



Name

Enter the name you wish to give to this pipe. You will refer to this name when creating links.

Bandwidth restriction

Determines whether there is a limit on the total concurrent bandwidth of this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

NoBandwidth: there is no bandwidth available.

Total bandwidth limit (kbps)

Sets the limit on the total concurrent bandwidth of this pipe.

Bandwidth restriction

Determines whether there is a limit on the bandwidth of individual calls via this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

NoBandwidth: there is no bandwidth available.

Per call bandwidth limit (kbps)

Sets the limit on the bandwidth of individual calls via this pipe.

Create Pipe

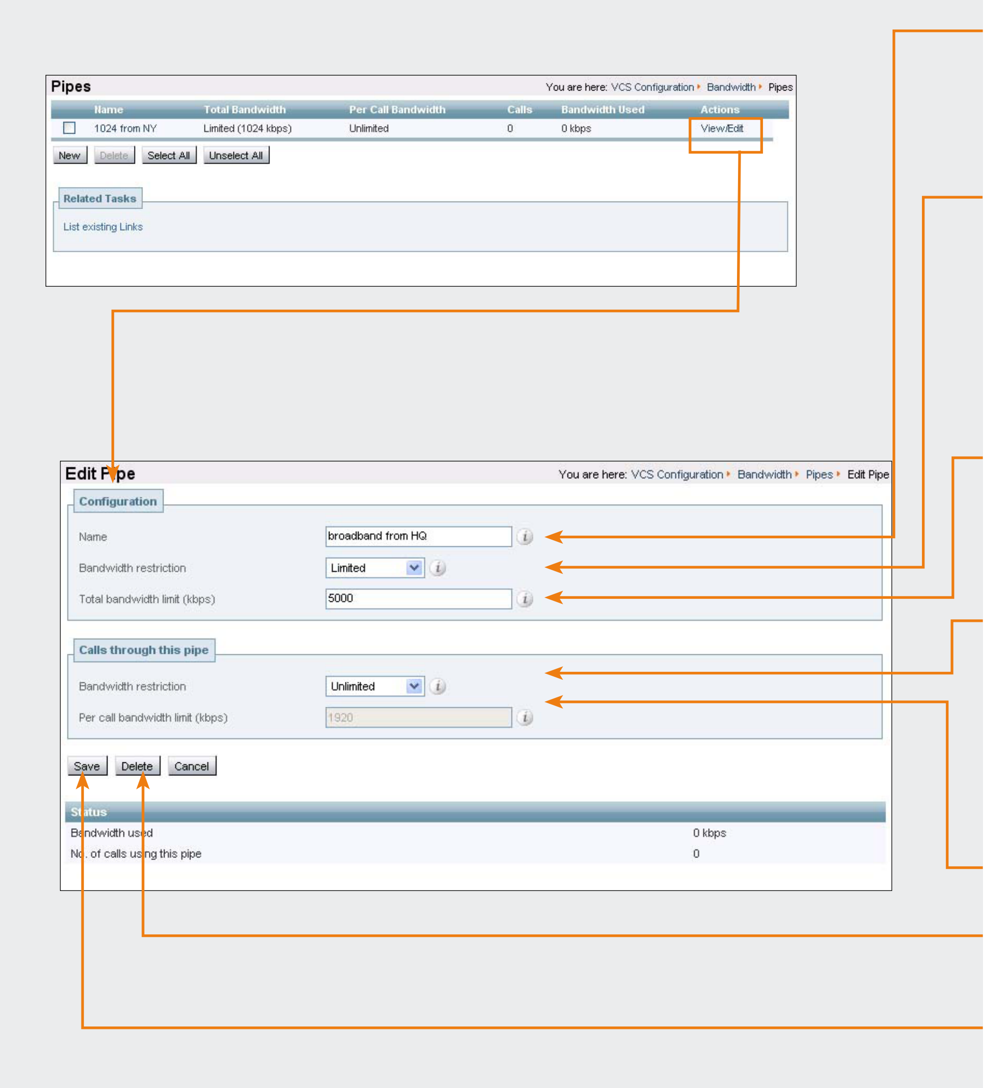
Click here to create the pipe and return to the Pipes page.

Editing Pipes

Editing an Existing Pipe

To configure details of a pipe:

- VCS Configuration > Bandwidth > Pipes
  You will be taken to the Pipes page.
  Click on the pipe you wish to configure.
  You will be taken to the Edit Pipe page.
- `xConfiguration Bandwidth Pipe`



Name

Enter the name you wish to give to this pipe. You will refer to this name when creating links.

Bandwidth restriction

Determines whether there is a limit on the total concurrent bandwidth of this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

NoBandwidth: there is no bandwidth available.

Total bandwidth limit (kbps)

Sets the limit on the total concurrent bandwidth of this pipe.

Bandwidth restriction

Determines whether there is a limit on the bandwidth of individual calls via this pipe.

Unlimited: no limitations are in place.

Limited: there is a limit in place; you must enter the limit in the field below.

NoBandwidth: there is no bandwidth available.

Per call bandwidth (kbps)

Sets the limit on the bandwidth of individual calls via this pipe.

Delete

Click here to delete the pipe.

Save

Click here to save the changes.

Applying Pipes to Links

Pipes are used to restrict the bandwidth of a link. When a pipe is applied to a link, it will restrict the bandwidth of calls made between the two nodes of the link - the restrictions will apply to calls in either direction.

Normally a single pipe would be applied to a single link. However, one or more pipes may be applied to one or more links, depending on how you wish to model your network.

One Pipe, One Link

Applying a single pipe to a single link is useful when you wish to apply specific limits to calls between a subzone and another specific subzone or zone.

One Pipe, Two or More Links

Each pipe may be applied to multiple links. This is used to model the situation where one site communicates with several other sites over the same broadband connection to the Internet. A pipe should be configured to represent the broadband connection, and then applied to all the links. This will allow you to configure the bandwidth options for calls in and out of that site.

Example

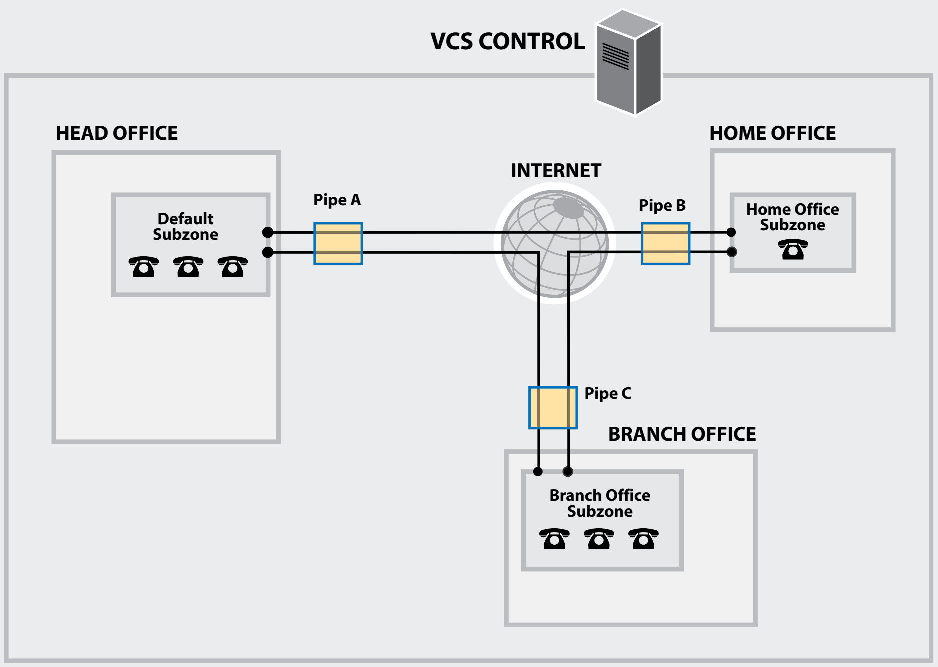
In the diagram opposite, Pipe A has been applied to two links: the link between the Default Subzone and the Home Office subzone, and the link between the Default Subzone and the Head Office subzone. In this case, Pipe A represents the Head Office's broadband connection to the internet, and would have total and per-call restrictions placed on it.

Two Pipes, One Link

Each link may have up to two pipes associated with it. This is used to model the situation where the two nodes of a link are not directly connected, for example two sites that each have their own broadband connection to the Internet. Each connection should have its own pipe, meaning that a link between the two nodes should be subject to the bandwidth restrictions of both pipes.

Example

In the diagram opposite, the link between the Default Subzone and the Home Office Subzone has two pipes associated with it: Pipe A, which represents the Head Office's broadband connection to the internet, and Pipe B, which represents the Home Office's dial-up connection to the internet. Each pipe would have bandwidth restrictions placed on it to represent its maximum capacity, and a call placed via this link would have the lower of the two bandwidth restrictions applied.



Default Bandwidth and Downspeeding

About the Default Call Bandwidth

Usually, when a call is initiated the endpoint will include in the request the amount of bandwidth it wishes to use. For those cases where the endpoint has not specified the bandwidth, you can set the VCS to apply a default bandwidth value.

About Downspeeding

If bandwidth control is in use, there may be situations when there is insufficient bandwidth available to place a call at the requested rate. By default (and assuming that there is some bandwidth still available) the VCS will still attempt to connect the call, but at a reduced bandwidth – this is known as downspeeding.

Downspeeding can be configured so that it is applied in either or both of the following scenarios:

- when the requested bandwidth for the call exceeds the lowest per-call limit for the subzone or pipe(s)
- when placing the call at the requested bandwidth would mean that the total bandwidth limits for that subzone or pipe(s) would be exceeded.

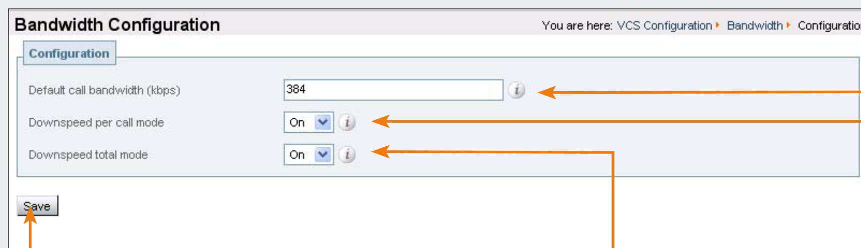
You can turn off downspeeding, in which case if there is insufficient bandwidth to place the call at the originally requested rate, the call will not be placed at all. This could be used if, when your network is nearing capacity, you would rather a call failed to connect at all than was connected at a lower than requested speed. In this situation users will get one of the following messages, depending on the message that initiated the search:

- `Exceeds Call Capacity`
- `Gatekeeper Resources Unavailable`

Configuring Default Call Bandwidth and Downspeeding

The default call bandwidth and downspeeding behavior are configured via:

- VCS Configuration > Bandwidth > Configuration.
  You will be taken to the Bandwidth Configuration page.
- `xConfiguration Bandwidth Default`
- `xConfiguration Bandwidth Downspeed`



Default call bandwidth (kbps)

Enter the bandwidth value to be used for calls for which no bandwidth value has been specified by the system that initiated the call.

This value cannot be blank. The default value is 384 kbps.

Downspeed per call mode

Determines what will happen if the per-call bandwidth restrictions on a subzone or pipe mean that there is insufficient bandwidth available to place a call at the requested rate.

On: the call will be downspeeded.

Off: the call will not be placed.

Save

Click here to save your changes

Downspeed total mode

Determines what will happen if the total bandwidth restrictions on a subzone or pipe mean that there is insufficient bandwidth available to place a call at the requested rate.

On: the call will be downspeeded.

Off: the call will not be placed.

Bandwidth Control Examples

Example Without a Firewall

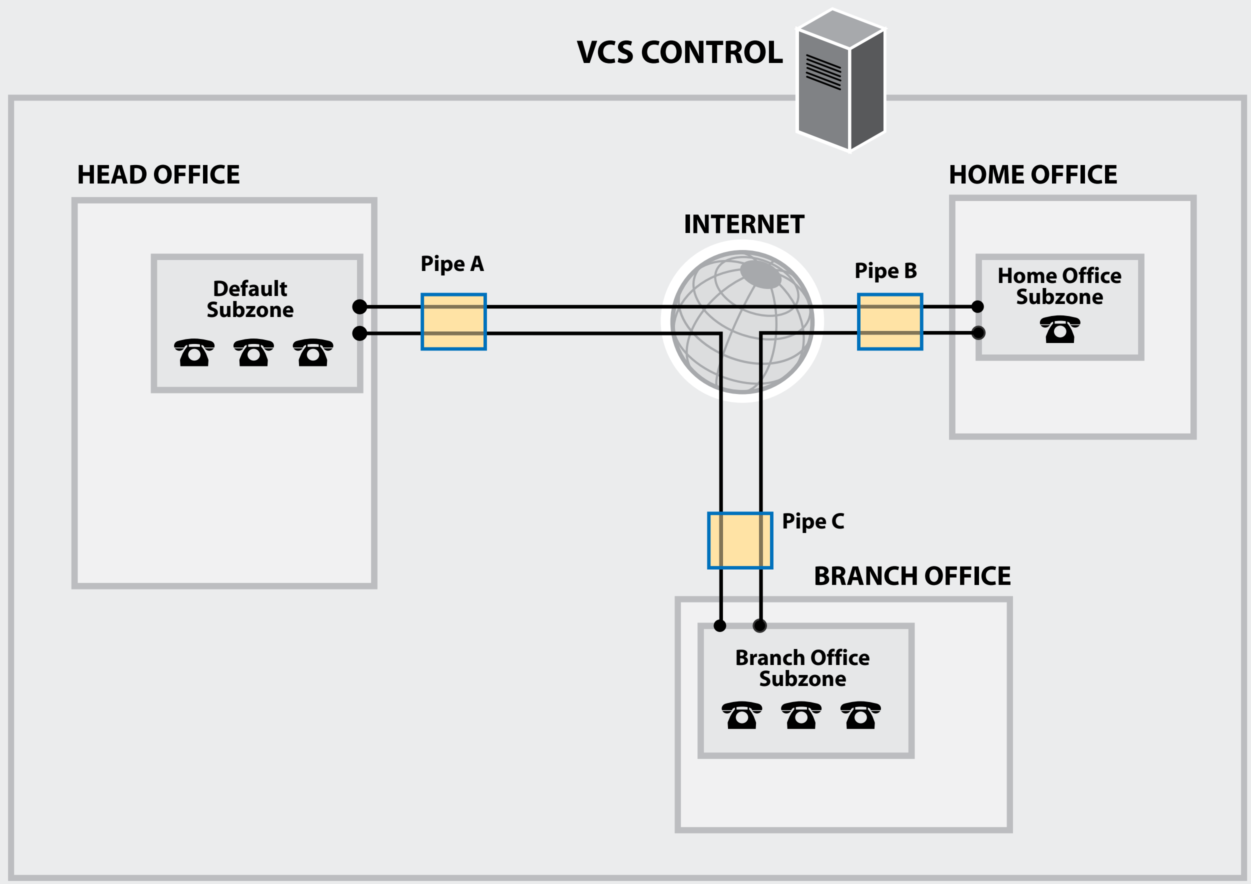
An example deployment is shown opposite. In this example, there are three geographically separate offices: Enterprise, Branch and Home. All endpoints in the Enterprise office register with the VCS Control, as do those in the Branch and Home offices.

Each of the three offices is represented as a separate subzone on the VCS, with bandwidth configured according to local policy.

The enterprise's leased line connection to the Internet, and the DSL connections to the remote offices are modeled as separate pipes.

There are no firewalls involved in this scenario, so we can configure direct links between each of the offices. Each link is then assigned two pipes, representing the Internet connections of the offices at each end of the link.

In this scenario, a call placed between the Home Office and Branch Office will consume bandwidth from the Home and Branch subzones and on the Home and Branch pipes. The Enterprise's bandwidth budget will be unaffected by the call.



Bandwidth Control Examples

Example With a Firewall

If we modify the previous example deployment to include firewalls between the offices, we can use TANDBERG's Expressway™ firewall traversal solution to maintain connectivity. We do this by adding a VCS Expressway outside the firewall on the public internet, which will work in conjunction with the VCS Control and Home and Branch office endpoints to traverse the firewalls.

In this example, the endpoints in the Head Office register with the VCS Control, whilst those in the Branch and Home offices register with the VCS Expressway.

The introduction of the firewalls means that there is no longer any direct connectivity between the Branch and Home offices. All traffic must be routed through the VCS Expressway. This is shown by the absence of a link between the Home and Branch subzones.

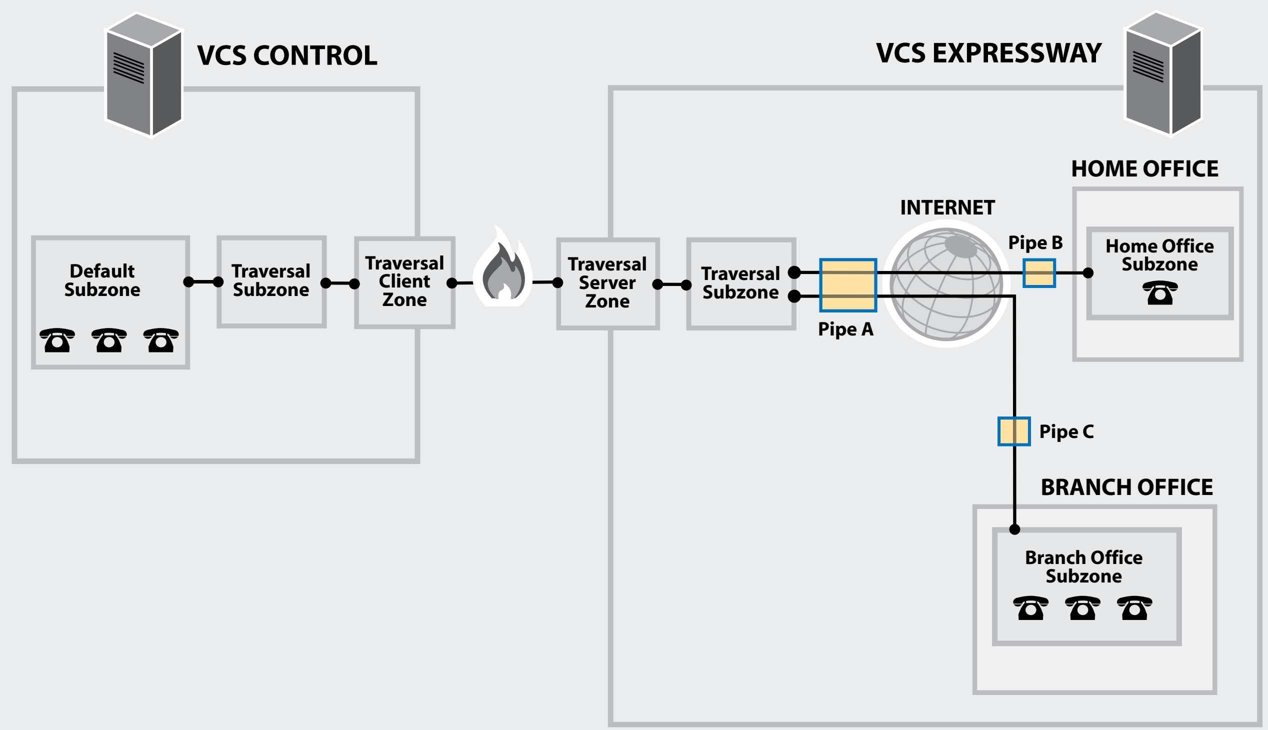
VCS Expressway Subzone Configuration

The VCS Expressway has subzones configured for the Home Office and Branch Office. These are linked to the VCS Expressway's Traversal Subzone, with pipes placed on each link. All calls from the VCS Expressway to the VCS Control must go through the Traversal Subzone and will consume bandwidth from this Subzone. Note also that calls from the Home Office to the Branch Office must also go through the Traversal Subzone, and will also consume bandwidth from this Subzone as well as the Home and Branch subzones and Home Office, Branch office and Head Office pipes.

In this example we have assumed that there is no bottleneck on the link between the VCS Expressway and the Head Office network, so have not placed a pipe on this link. If you want to limit the amount of traffic flowing through your firewall, you could provision a pipe on this link.

VCS Control Subzone Configuration

Because the VCS Control is only managing endpoints on the Head Office LAN, its configuration is simpler. All of the endpoints in the Head Office are assigned to the Default Subzone. This is linked to the Traversal Subzone, through which all calls leaving the Head Office must pass.



Firewall Traversal

This section describes how to configure your VCS Control and VCS Expressway in order to traverse firewalls. It also describes how to configure the additional firewall traversal server functions of a VCS Expressway, including STUN services.



Firewall Traversal Overview

About Expressway™

The purpose of a firewall is to control the IP traffic entering your network. Firewalls will generally block unsolicited incoming requests, meaning that any calls originating from outside your network will be prevented. However, firewalls can be configured to allow outgoing requests to certain trusted destinations, and to allow responses from those destinations. This principle is used by TANDBERG's Expressway™ solution to enable secure traversal of any firewall.

The Expressway™ solution consists of:

1. a TANDBERG VCS Expressway or TANDBERG Border Controller located outside the firewall on the public network or in the DMZ, which acts as the firewall traversal server
2. a TANDBERG VCS Control, TANDBERG Gatekeeper, MXP endpoint or other traversal-enabled endpoint located in a private network, which acts as the firewall traversal client.

The two systems work together to create an environment where all connections between the two are outbound, i.e. established from the client to the server, and thus able to successfully traverse the firewall.

How does it work?

The traversal client constantly maintains a connection via the firewall to a designated port on the traversal server. This connection is kept alive by the client sending packets at regular intervals to the server. When the traversal server receives an incoming call for the traversal client, it uses this existing connection to send an incoming call request to the client. The client then initiates the necessary outbound connections required for the call media and/or signaling.

This process ensures that from the firewall's point of view, all connections are initiated from the traversal client inside the firewall out to the traversal server.

VCS as a Firewall Traversal Client

Your VCS can act as a firewall traversal client on behalf of SIP and H.323 endpoints registered to it, and any gatekeepers that are neighbored with it.

In order to act as a firewall traversal client, the VCS must be configured with information about the system(s) that will be acting as its firewall traversal server. See the section on Configuring the VCS as a Traversal Client for full details on how to do this.

In most cases, you will use a VCS Control as a firewall traversal client. However, a VCS Expressway can also act as a firewall traversal client.

The firewall traversal server used by the VCS client can be a TANDBERG VCS Expressway, or (for H.323 only) a TANDBERG Border Controller.

VCS as a Firewall Traversal Server

The VCS Expressway has all the functionality of a VCS Control (including being able to act as a firewall traversal client). However, its main feature is that it can act as a firewall traversal server for other TANDBERG systems and any traversal-enabled endpoints that are registered directly to it. It can also provide STUN Discovery and STUN relay services to endpoints with STUN clients. These features are enabled as follows:

- In order for the VCS Expressway to act as a firewall traversal server for TANDBERG systems, you must create and configure a new traversal server zone on the VCS Expressway for every system that is its traversal client. See Configuring the VCS as a Traversal Server for full instructions.
- In order for the VCS Expressway to act as a firewall traversal server for traversal-enabled endpoints (i.e. TANDBERG MXP endpoints and any other endpoints that support the ITU H.460.18 and H.460.19 standards), no additional configuration is required. See Configuring Traversal for Endpoints for more information on the options available.
- To enable STUN Discovery and STUN Relay services, see STUN Services.
- To reconfigure the default ports used by the VCS Expressway, see Configuring Traversal Server Ports.

In order for firewall traversal to function correctly, the VCS Expressway must have one traversal server zone configured on it for each client system that is connecting to it (this does not include traversal-enabled endpoints which register directly with the VCS Expressway; the settings for these connections are configured in a different way). Likewise, each VCS client must have one traversal client zone configured on it for each server that it is connecting to. The ports and protocols configured for each pair of client-server zones must be the same. (See Quick Guide to VCS Traversal Client - Server Configuration for a summary of the configuration on each system.) Because the VCS Expressway listens for connections from the client on a specific port, we recommend that you create the traversal server zone on the VCS Expressway before you create the traversal client zone on the VCS Control.

Quick Guide to VCS Traversal Client - Server Configuration

Overview	VCS Control (Client)	VCS Expressway (Server)

Full details of how to configure a VCS Control and VCS Expressway as traversal client and server respectively are given in the following pages. However, the basic steps are:

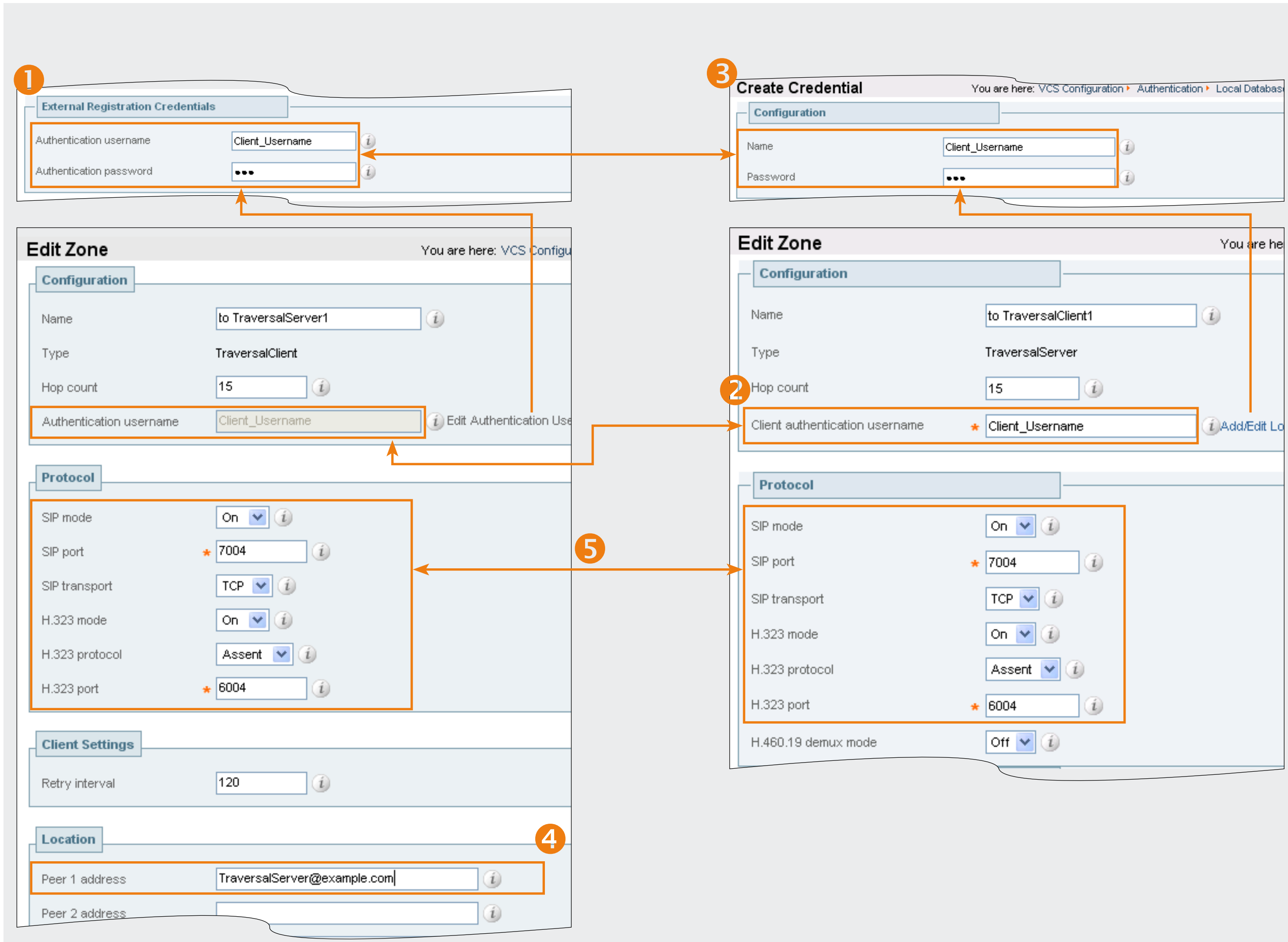
1. Ensure the VCS Control has been configured with an Authentication username and Authentication password to use as its External Registration Credentials. These can be added or edited via VCS Configuration > Authentication > Configuration (or by clicking on the Edit Authentication Username/Password link in the Edit Zone page for an existing Traversal Client Zone).

2. On the VCS Expressway, create a Traversal Server Zone (this represents the incoming connection from the VCS Control). In the Client authentication username field, enter the VCS Control's Authentication username.

3. On the VCS Expressway, add the VCS Control's authentication username and password as credentials in the authentication database. These can be added or edited via VCS Configuration > Authentication > Local Database, or by clicking on the Add/Edit Local Authentication Database link in the Edit Zone page.

4. On the VCS Control, create a Traversal Client Zone (this represents the connection to the VCS Expressway). Enter the VCS Expressway's IP address or FQDN in the Peer 1 address field.

5. On the VCS Control, configure all the modes and ports in the Protocol section to match identically those of the Traversal Server Zone on the VCS Expressway.



Firewall Traversal Protocols and Ports

Overview

Ports play a vital part in firewall traversal configuration. The correct ports must be set on the VCS Expressway, traversal client and firewall in order for connections to be permitted.

Ports are initially configured on the VCS Expressway by the VCS Expressway Administrator. The firewall administrator and the traversal client administrator should then be notified of the ports, and they then must then configure their systems to connect to these specific ports on the server. The only port configuration that is done on the client is the range of ports it uses for outgoing connections; the firewall administrator may need to know this information so that if necessary they can configure the firewall to allow outgoing connections from those ports.

Expressway Process

The Expressway™ solution works as follows:

1. Each traversal client connects via the firewall to a unique port on the VCS Expressway.
2. The server identifies each client by the port on which it receives the connection, and the Authentication credentials provided by the client.
3. Once established, the client constantly sends a probe to the VCS Expressway via this connection in order to keep the connection alive.
4. When the VCS Expressway receives an incoming call for the client, it uses this initial connection to send an incoming call request to the client.
5. The client then initiates one or more outbound connections. The destination ports used for these connections will differ for signaling and/or media, and will depend on the protocol being used (see the following sections for more details).

H.323 Firewall Traversal Protocols

The VCS supports two different firewall traversal protocols for H.323: Assent and H.460.18/H.460.19.

- Assent is TANDBERG's proprietary protocol.
- H.460.18 and H.460.19 are ITU standards which define protocols for the firewall traversal of signaling and media respectively. These standards are based on the original TANDBERG Assent protocol.

In order for a traversal server and traversal client to communicate, they must be using the same protocol.

The two protocols each use a slightly different range of ports.

SIP Firewall Traversal Protocols

The VCS supports the Assent protocol for SIP firewall traversal of media.

The signaling is traversed through TCP/TLS connection established from the client to the server.

Firewall Traversal Protocols and Ports

Ports for Initial Connections from Traversal Clients

Each traversal server zone specifies an H.323 port and a SIP port to be used for the initial connection from the client.

Each time you configure a new traversal server zone on the VCS Expressway, you will be allocated default port numbers for these connections:

- H.323 ports will start at UDP/6001 and increment by 1 for every new traversal server zone
- SIP ports will start at TCP/7001 and increment by 1 for every new traversal server zone.

You can change these default ports if necessary but you must ensure that the ports are unique for each traversal server zone.

Once the H.323 and SIP ports have been set on the VCS Expressway, matching ports must be configured on the corresponding traversal client.

You must allow outbound connections through your firewall to each of the unique SIP and H.323 ports that are configured on each of the VCS Expressway's traversal server zones.

The default port used for the initial connections from MXP endpoints is the same as that used for standard RAS messages, i.e. UDP/1719. While it is possible to change this port on the VCS Expressway, most endpoints will not support connections to ports other than UDP/1719. We therefore recommend that this be left as the default.

Assent Ports

For connections to the VCS Expressway using the Assent protocol, the default ports are:

Call signaling

- UDP/1719: listening port for RAS messages
- TCP/2776: listening port for H.225 and H.245 protocols

Media

- UDP/2776: RTP media port
- UDP/2777: RTCP media control port

H.460.18/19 Ports

For connections to the VCS Expressway using the H.460.18/19 protocols, the default ports are:

Call signaling

- UDP/1719: listening port for RAS messages
- TCP/1720: listening port for H.225 protocol
- TCP/2777: listening port for H.245 protocol

Media

- UDP/2776: RTP media port
- UDP/2777: RTCP media control port

If your VCS Expressway does not have any endpoints registering directly with it, and it has no Alternates configured, then UDP/1719 is not required. You therefore do not need to allow outbound connections to this port through the firewall between the VCS Control and VCS Expressway.

SIP Ports

Call signaling

SIP call signaling uses the same port as used by the initial connection between the client and server.

Media

Where the traversal client is a VCS, SIP media uses Assent to traverse the firewall . The default ports are the same as for H.323, i.e.:

- UDP/2776: RTP media port
- UDP/2777: RTCP media control port

STUN Ports

The VCS Expressway can be enabled to provide STUN services (STUN Relay and STUN Binding Discovery) which can be used by SIP endpoints which support the ICE firewall traversal protocol.

The ports used by these services are configurable via:

- VCS Configuration > Expressway > STUN
- `xConfiguration Traversal Server STUN`

The ICE clients on each of the SIP endpoints must be able to discover these ports, either via SRV records in DNS or by direct configuration.

Ports for Connections out to the Public Internet

In situations where the VCS Expressway is attempting to connect to an endpoint on the public internet, you will not know the exact port(s) on the endpoint to which the connection will be made. This is because the ports to be used are determined by the endpoint and advised to the VCS Expressway only once the server has located the endpoint on the public internet. This may cause problems if your VCS Expressway is located within a DMZ (i.e. there is a firewall between the VCS Expressway and the public internet) as you will not be able to specify in advance rules that will allow you to connect out to the endpoint's ports.

You can however specify the ports on the VCS Expressway that will be used for calls to and from endpoints on the public internet so that your firewall administrator can allow connections via these ports. The ports that can be configured for this purpose are:

H.323

- TCP/1720: signaling
- UDP/1719: signaling
- UDP/50,000-51199: media
- TCP/15,000-19999: signaling

SIP

- TCP/5061: signaling
- UDP/5060 (default): signaling
- UDP/50,000-51199: media
- TCP: a temporary port in the range 25000-29999 is allocated.

STUN

- 3478/UDP (default): STUN Discovery
- 4678/UDP: (default): STUN Relay
- 60000-61200/UDP (default range): media

Firewall Traversal and Authentication

Overview

In order to control which systems can use the VCS Expressway as a traversal server, each VCS Control or Gatekeeper that wishes to be its client must first authenticate with it.

Upon receiving the initial connection request from the traversal client, the VCS Expressway asks the client to authenticate itself by providing a username and password. The VCS Expressway then looks up the client's username and password in its own authentication database. If a match is found, the VCS Expressway will accept the request from the client.

The settings used for authentication depend on the combination of client and server being used. These are detailed in the table opposite.

All VCS and Gatekeeper traversal clients must authenticate with the VCS Expressway, regardless of the VCS Expressway's Authentication Mode setting. However, endpoint clients are only required to authenticate if the VCS Expressway's Authentication Mode is On.

Authentication and NTP

All VCS and Gatekeeper traversal clients must authenticate with the VCS Expressway. The authentication process makes use of timestamps and requires that each system is using an accurate system time. The system time on a VCS is provided by a remote NTP server. Therefore, in order for firewall traversal to work, all systems involved must be configured with details of an NTP server.

Client	Server
VCS Control or VCS Expressway • The VCS client provides its Authentication Username and Authentication Password. These are set on the VCS client via VCS Configuration > Authentication > Configuration, in the External Registration Credentials section.	VCS Expressway • The traversal server zone for the VCS client must be configured with the Client Authentication Username. This is set on the VCS Expressway via VCS Configuration > Zones > Edit Zone, in the Configuration section. • There must also be an entry in the VCS Expressway's authentication database with the corresponding client username and password.
Endpoint • The endpoint client provides its Authentication ID and Authentication Password.	VCS Expressway • There must be an entry in the VCS Expressway's authentication database with the corresponding client username and password.
TANDBERG Gatekeeper (version 5.2 and earlier) • The Gatekeeper looks up its System Name in its own authentication database and retrieves the password for that name. It then provides this name and password.	VCS Expressway • The traversal server zone for the Gatekeeper client must be configured with the Gatekeeper's System Name in the Client Authentication Username field. This is set on the VCS Expressway via VCS Configuration > Zones > Edit Zone, in the Configuration section. • There must be an entry in the VCS Expressway's authentication database that has the Gatekeeper's System name as the username, along with the corresponding password.
TANDBERG Gatekeeper (version 6.0 and later) • The Gatekeeper provides its Authentication Username and Authentication Password. These are set on the Gatekeeper via Gatekeeper Configuration > Authentication, in the External Registration Credentials section.	VCS Expressway • The traversal server zone for the Gatekeeper client must be configured with the Gatekeeper's Authentication Username. This is set on the VCS Expressway via VCS Configuration > Zones > Edit Zone, in the Configuration section • There must also be an entry in the VCS Expressway's authentication database with the corresponding client username and password.
VCS Control or VCS Expressway • If Authentication is On on the Border Controller, the VCS client provides its Authentication Username and Authentication Password. These are set on the VCS client via VCS Configuration > Authentication > Configuration, in the External Registration Credentials section. • If the Border Controller is in Assent mode, the VCS client provides its Authentication Username. This is set on the VCS client via VCS Configuration > Authentication > Configuration, in the External Registration Credentials section.	Border Controller • If Authentication is On on the Border Controller, there must be an entry in the Border Controller's authentication database that matches the VCS client's Authentication Username and Authentication Password. • If the Border Controller is in Assent mode, the traversal zone configured on the Border Controller to represent the VCS client must use the VCS's Authentication Username in the Assent Account name field. This is set on the Border Controller via TraversalZone > Assent > Account name.

Firewall Traversal and Dual Network Interfaces

The Dual Network Interfaces option enables the LAN 2 interface on your VCS Expressway (the option is not available on a VCS Control). The LAN 2 interface is used in situations where your VCS Expressway is located in a DMZ that consists of two separate networks - an inner DMZ and an outer DMZ - and your firewall rules prevent communication between the two.

With the LAN 2 interface enabled, you can configure the VCS with two separate IP addresses, one for each network in the DMZ. Your VCS then acts as a proxy server between the two networks, allowing calls to pass between the internal and outer firewalls that make up your DMZ.

All ports configured on the VCS, including those relating to firewall traversal, will apply to both IP addresses; it is not possible to configure these ports separately for each IP address.

Firewall Configuration

In order for Expressway™ firewall traversal to function correctly, the firewall must be configured to:

- allow initial outbound traffic from the client to the ports being used by the VCS Expressway
- allow return traffic from those ports on the VCS Expressway back to the originating client.

TANDBERG offers a downloadable tool, the Expressway Port Tester, that allows you to test your firewall configuration for compatibility issues with your network and endpoints. It will advise if necessary which ports may need to be opened on your firewall in order for the Expressway™ solution to function correctly. The Expressway Port Tester currently only supports H.323. Contact your TANDBERG representative for more information.

We recommend that you turn off any H.323 and SIP protocol support on the firewall: these are not needed in conjunction with the TANDBERG Expressway™ solution and may interfere with its operation.

Configuring the VCS as a Traversal Client

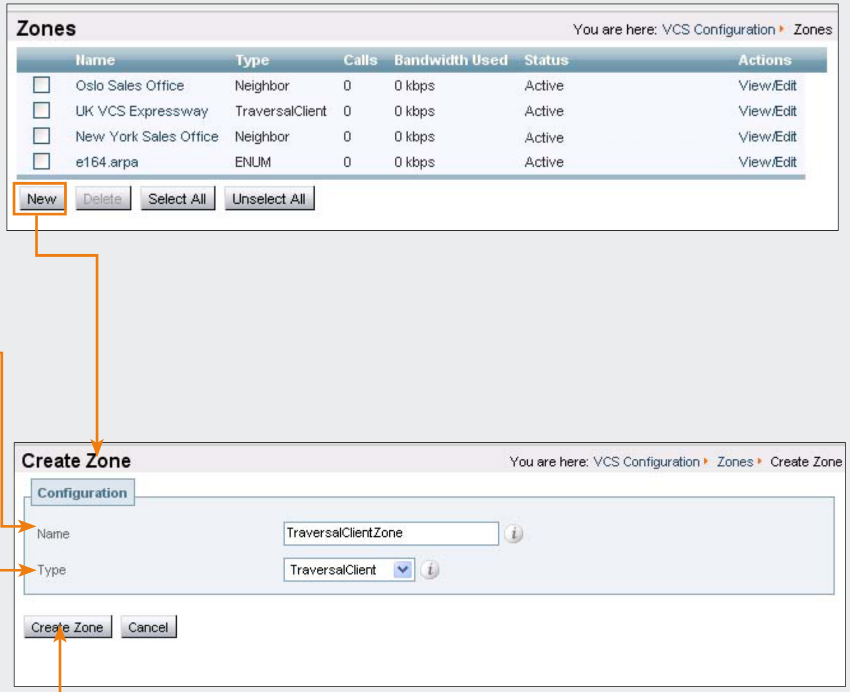
Overview

To enable your VCS to act as a traversal client on behalf of its endpoints and neighbor gatekeepers, you must create a connection between it and a traversal server (e.g. a TANDBERG VCS Expressway or Border Controller).

You do this by adding a new traversal client zone on the VCS client and configuring it with the details of the traversal server.

Adding a New Traversal Client Zone

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Select New.
  You will be taken to the Create Zone page.
- xCommand ZoneAdd



Name

Enter the name you wish to give to this zone. The name acts as a unique identifier, allowing you to distinguish between zones of the same type.

Type

From the Type drop-down menu, select TraversalClient.

Create Zone

Click here to create the zone. You will be taken directly to the Edit Zone page, where you can configure the traversal client zone as required.

You can create more than one traversal client zone if you wish to connect to multiple traversal servers.

Configuring the VCS as a Traversal Client

Configuring a Traversal Client Zone

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zone page.
- xConfiguration Zones Zone [1..200]
- xConfiguration Zones Zone [1..200] Traversal Client

Hop count

Specifies the hop count to be used when querying this zone.

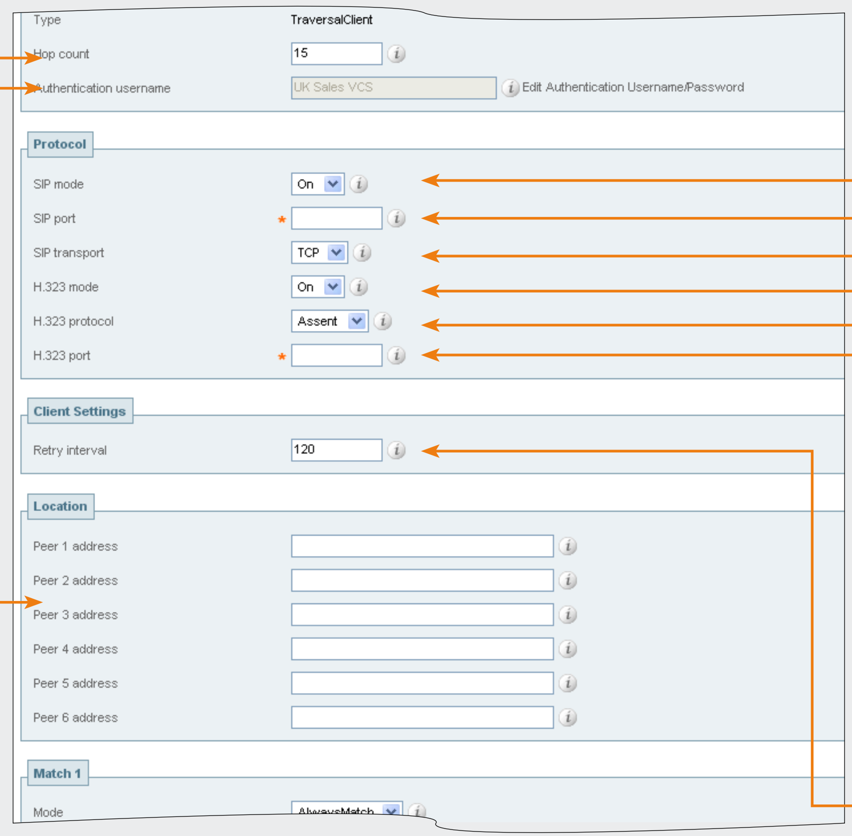
Authentication username

This field displays the Authentication username that has been configured on this VCS. The Authentication username and password are system-wide settings that are used for all Traversal Client Zones. The Authentication username cannot be edited directly from this page but it is shown here for reference as it is needed when configuring the corresponding Traversal Server Zone.

To edit the Authentication username, click on the Edit Authentication Username/Password link. This will take you to the Authentication page, where you can edit the settings under the External Registration Credentials section.

Peer 1 to Peer 6 address

The IP Address or FQDN of the traversal server. If the traversal server is a VCS cluster, this includes all of its Peers. See the section Neighboring the Local VCS to a Cluster for more information.



SIP mode

Determines whether SIP calls will be allowed to and from this zone.

SIP port

Specifies the port on the traversal server to be used for SIP calls from this VCS.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal server.

H.323 mode

Determines whether H.323 calls will be allowed to and from this zone.

H.323 protocol

Determines which of the two firewall traversal protocols to use for calls to the traversal server.

H.323 port

Specifies the port on the traversal server to be used for H.323 firewall traversal calls.

Retry interval

Specifies the interval in seconds with which a failed attempt to establish a connection to the traversal server should be retried.

Remember to Save your changes.

Configuring the VCS as a Traversal Server

Overview

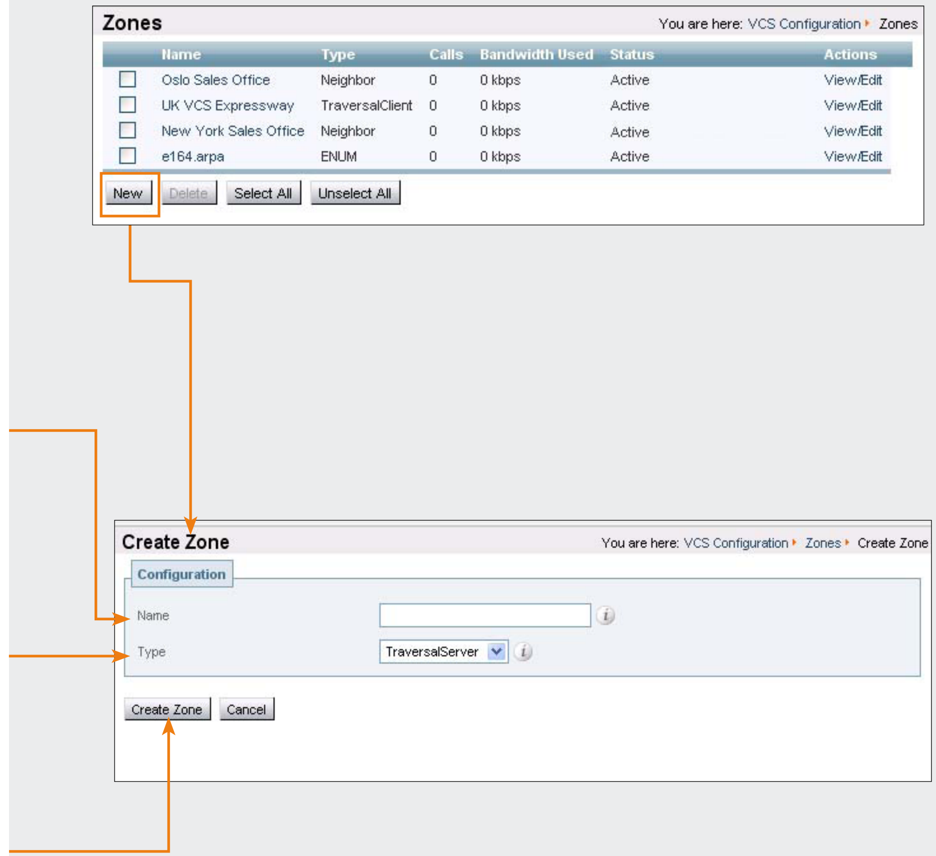
The VCS Expressway can act as a firewall traversal server. This feature means you can:

- Allow your VCS to act as a traversal server for other VCSs and TANDBERG Gatekeepers. You do this by adding a new traversal server zone on the VCS, and configuring it with details of the traversal client.
- Provide firewall traversal for any traversal-enabled endpoints (i.e. TANDBERG MXP endpoints and any other endpoints that support the ITU H.460.18 and H.460.19 standards) registered directly with it. You can configure the protocols and ports that will be used.
- Enable and configure STUN services.
- Configure the ports used specifically for firewall traversal services.

The following sections describe how to configure each of the above options.

Adding a New Traversal Server Zone

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Select New.
  You will be taken to the Create Zone page.
- `xCommand ZoneAdd`



Name

Enter the name you wish to give to this zone. The name acts as a unique identifier, allowing you to distinguish between zones.

Type

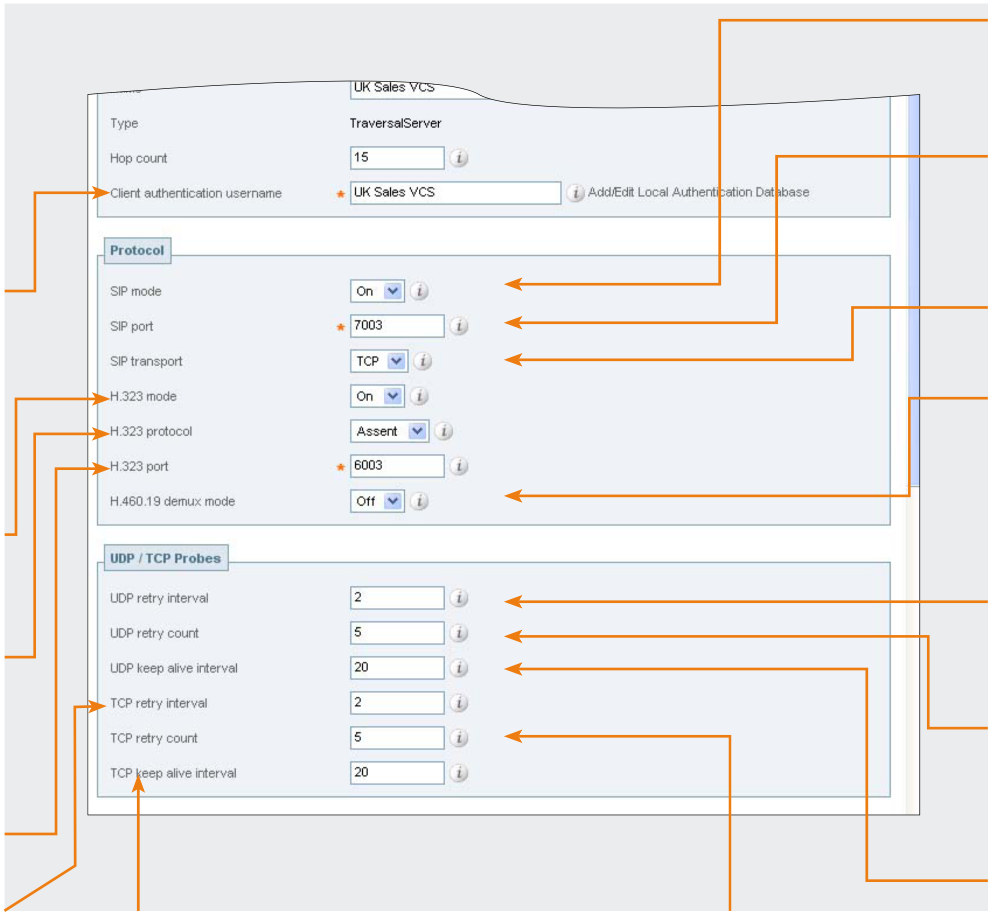
From the Type drop-down menu, select TraversalServer.

Create Zone

Click here to create the zone. You will be taken directly to the Edit Zone page, where you can configure the traversal server zone as required.

Configuring a Traversal Server Zone

- VCS Configuration > Zones.
  You will be taken to the Zones page.
  Click on the name of the zone you wish to configure.
  You will be taken to the Edit Zones page.
- xConfiguration Zones Zone
- xConfiguration Zones Zone [1..200] TraversalServer



Client authentication username

If the traversal client is a VCS, this must be the VCS's Authentication Username.

You must also add the client's Authentication username and password to the VCS's authentication database. To go directly to the page where you can do this, click on the Add/Edit Local Authentication Database link.

H.323 mode

Determines whether H.323 calls will be allowed to and from the traversal client.

H.323 protocol

Determines which of the two firewall traversal protocols will be used for calls through the firewall, to and from the client. The same protocol must be used by the client.

H.323 port

Specifies the port on the VCS Expressway to be used for H.323 connections from the client.

TCP retry interval

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS Expressway.

TCP keep alive interval

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

TCP retry count

Sets the number of times the traversal client will attempt to send a TCP probe to the VCS Expressway.

SIP mode

Determines whether SIP calls will be allowed to and from the traversal client.

SIP port

Specifies the port on the VCS Expressway to be used for SIP calls from the traversal client.

SIP transport

Determines which transport type will be used for SIP calls to and from the traversal client.

H.460.19 demux mode

On: allows use of the same two ports for media for all calls from the traversal client.

Off: each call from the traversal client will use a separate pair of ports for media.

UDP retry interval

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS Expressway.

UDP retry count

Sets the number of times the traversal client will attempt to send a UDP probe to the VCS Expressway.

UDP keep alive interval

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.

Configuring the VCS as a Traversal Server

Configuring Traversal for Endpoints

Overview

Traversal-enabled H.323 endpoints can register directly with the VCS Expressway and use it for firewall traversal.

To configure the options for these endpoints:

- VCS Configuration > Expressway> Locally Registered Endpoints
  You will be taken to the Locally Registered Endpoints page.
- xConfiguration Zones LocalZone Traversal H323

H.323 Assent mode

Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed.

H.460.18 mode

Determines whether or not H.323 calls using H.460.18/19 mode for firewall traversal will be allowed.

H.460.19 demux mode

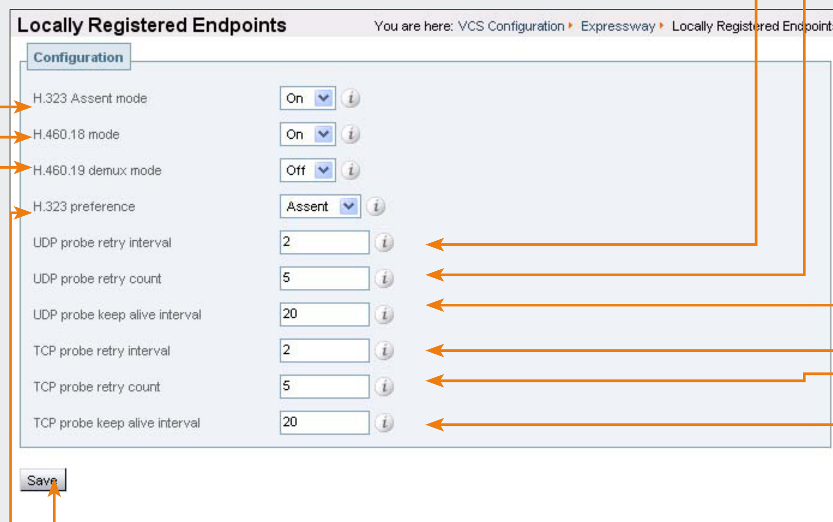
Determines whether the VCS Expressway will operate in Demultiplexing mode for calls from locally registered endpoints.

On: allows use of the same two ports for all calls.

Off: Each call will use a separate pair of ports for media.

H.323 preference

If an endpoint supports both Assent and H.460.18 protocols, this setting determines which the VCS Expressway uses.



UDP probe retry interval

Sets the frequency (in seconds) with which locally registered endpoints will send a UDP probe to the VCS Expressway.

UDP probe retry count

Sets the number of times locally registered endpoints will attempt to send a UDP probe to the VCS Expressway.

UDP probe keep alive interval

Sets the interval (in seconds) with which locally registered endpoints will send a UDP probe to the VCS Expressway once a call is established, in order to keep the firewall's NAT bindings open.

TCP probe retry interval

Sets the frequency (in seconds) with which locally registered endpoints will send a TCP probe to the VCS Expressway.

TCP probe retry count

Sets the number of times locally registered endpoints will attempt to send a TCP probe to the VCS Expressway.

TCP probe keep alive interval

Sets the interval (in seconds) with which locally registered endpoints will send a TCP probe to the VCS Expressway once a call is established, in order to keep the firewall's NAT bindings open.

Save

Click here to save your settings.

Configuring the VCS as a Traversal Server

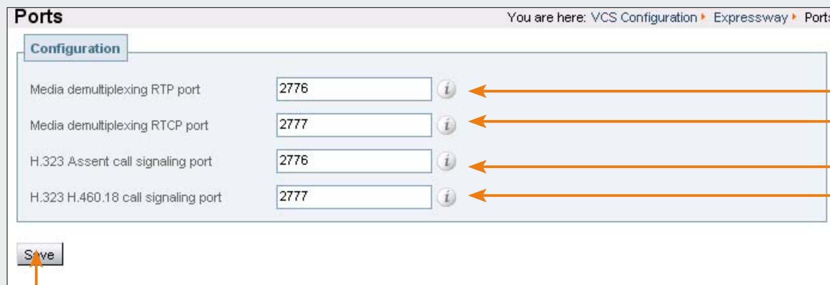
Configuring Traversal Server Ports

Overview

The VCS Expressway has specific listening ports used for firewall traversal. Rules must be set on your firewall to allow connections to these ports. In most cases the default ports should be used. However, you have the option to change these ports if necessary.

To configure the VCS Expressway ports:

- VCS Configuration > Expressway > Ports
  You will be taken to the Ports page.
- xConfiguration Traversal Server Media Demultiplexing
- xConfiguration Traversal Server H.323



Media demultiplexing RTP port

Specifies the port on the VCS to be used for demultiplexing RTP media.

Media demultiplexing RTCP port

Specifies the port on the VCS to be used for demultiplexing RTCP media.

H.323 Assent call signaling port

Specifies the port on the VCS to be used for Assent signaling.

H.323 H.460.18 call signaling port

Specifies the port on the VCS to be used for H.460.18 signaling.

Save

Click here to save your settings.

STUN Services

About STUN

STUN is a network protocol that enables a SIP or H.323 client to communicate via UDP or TCP from behind a NAT firewall.

The VCS Expressway can be configured to provide two types of STUN services to traversal clients. These services are STUN Binding Discovery and STUN Relay. Currently the VCS supports STUN over UDP only.

For detailed information on the base STUN protocol and the Binding Discovery service, refer to Session Traversal Utilities for (NAT) (STUN) [11].

For detailed information on the STUN Relay service, refer to Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN) [12].

About ICE

Currently, the most likely users of STUN services are ICE endpoints.

ICE (Interactive Connectivity Establishment) is a collaborative algorithm that works together with STUN services (and other NAT traversal techniques) to allow clients to achieve firewall traversal. The individual techniques on their own may allow traversal in certain network topologies but not others. Also some techniques maybe less efficient than others, involving extra hops (e.g. STUN Relay).

ICE involves the collecting of potential (candidate) points of contact (IP address and port combination) via each of the traversal techniques, the verification of peer-to-peer connectivity via each of these points of contact and then the selection of the "best" successful candidate point of contact to use.

STUN Binding Discovery

The STUN Binding Discovery service provides information back to the client about the binding allocated by the NAT firewall being traversed.

How it works

A client behind a NAT firewall sends a STUN discovery request via the firewall to the VCS Expressway, which has been configured as a STUN discovery server. Upon receipt of the message, the VCS Expressway responds to the client with information about the allocated NAT binding, i.e. the public IP address and the ports being used.

The client can then provide this information to other systems which may want to reach it, allowing it to be found even though it is not directly available on the public internet.

The endpoint will only be reachable if the firewall has the Endpoint-Independent Mapping behavior as described in RFC 4787 [13].

STUN Relay

The STUN Relay service (formerly known as TURN) allows a client to ask for data to be relayed to it from specific remote peers via the relay server and through a single connection between the client and the relay server.

How it works

A client behind a NAT firewall sends a STUN Allocate request to the VCS Expressway which is acting as the STUN relay server. The sending of this request opens a binding on the firewall. Upon receipt of the request, the VCS Expressway opens a public IP port on behalf of the client, and reports back to the client this IP address and port, as well as details of the firewall binding. The client can then provide this IP address and port to other systems which may want to reach it.

The client can restrict the remote address and ports from which the relay should forward on media. Any incoming calls to this IP address and port on the VCS server are relayed via the allocated binding on the NAT to the client.

STUN Relays consume traversal call licences (three relays take one licence) but they do not actually pass through the traversal subzone.

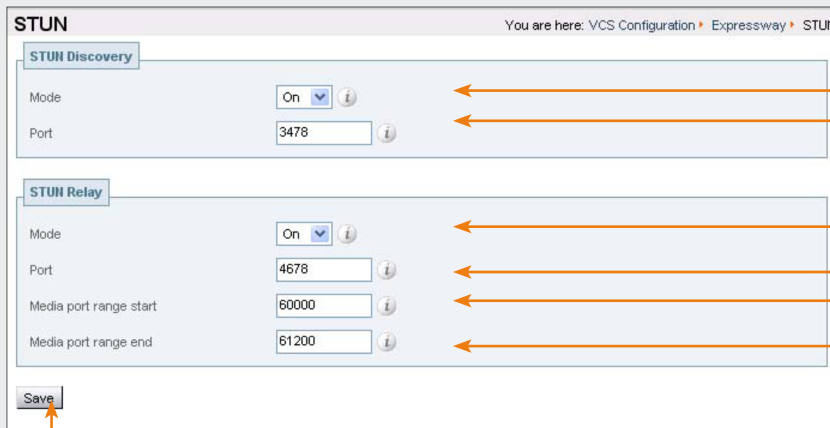
Configuring the VCS as a Traversal Server

STUN Services

Configuring STUN Services

To configure the STUN Binding Discovery and STUN Relay services:

- VCS Configuration > Expressway > STUN.
  You will be taken to the STUN page.
- xConfiguration Traversal Server STUN



STUN Discovery Mode

Determines whether the VCS will offer STUN Discovery services to traversal clients.

STUN Discovery Port

Specifies the port on the VCS on which it will be listening for STUN Discovery requests.

STUN Relay Mode

Determines whether the VCS will offer STUN Relay services to traversal clients.

STUN Relay Port

Specifies the port on the VCS on which it will be listening for STUN relay requests.

STUN Relay Media port range start

Specifies the lower port in the range to be used for STUN media relay.

STUN Relay Media port range end

Specifies the upper port in the range to be used for STUN media relay.

Save

Click here to save your changes.

Applications

This section provides information on each of the additional services that are available under the Applications menu of the VCS. You must purchase the appropriate option key in order to use each of these applications. They are:

- FindMe (User Policy)
- Presence Services



Overview

What is FindMe?

FindMe is a form of User Policy, which is the set of rules that determines what happens to a call for a particular user or group when it is received by the TANDBERG VCS.

The FindMe feature lets you assign a single "FindMe" name to individuals or groups in your enterprise. Users can determine which devices will be called when their FindMe name is dialed, and can also specify what happens if those devices are busy or go unanswered.

The FindMe feature means that potential callers can be given a single FindMe Alias on which they can contact an individual or group in your enterprise - callers won't have to know details of all the devices on which that person or group might be available.

To enable this feature you must purchase and install the appropriate option key. Contact your TANDBERG representative for information.

Process Overview

When the VCS receives a call for a particular alias, it checks to see whether User Policy has been enabled. If so, the VCS queries the User Policy Manager to see whether that alias is listed as a FindMe name. If so, the call is forwarded to the aliases according to configuration for that FindMe alias.

If User Policy has not been enabled, or the alias is not present in the User Policy Manager, the VCS will continue to search for the alias in the usual manner, i.e. first locally and then sending the request out to neighbors.

User Policy is invoked after any Administrator Policy configured on the VCS has been applied. See the Call Processing Diagram for more information.

Recommendations When Deploying FindMe

- The FindMe name should be in the form of a URI, and should be the individual's primary URI.
- Endpoints should not register with an alias that is the same as an existing FindMe name. You can prevent this by including all FindMe names on the Deny List.

Example

Users at Example Corp. have a FindMe name in the format john.smith@example.com. Each of the user's endpoints are registered with a slightly different alias that identifies its physical location. For example their office endpoint is registered with an alias in the format john.smith.office@example.com and their home endpoint as john.smith.home@example.com. Both of these endpoints are included in the list of devices to ring when the FindMe name is dialed. The alias john.smith@example.com is added to the Deny List, to prevent an individual endpoint registering with that alias.

How are Devices Specified?

When configuring their FindMe account, users are asked to specify the devices to which calls to their FindMe name will be routed.

It is possible to specify aliases and even other FindMe names as one or more of the devices. However, care must be taken in these situations to avoid circular configurations.

For this reason, we recommend that users specify the physical devices they wish to ring when their FindMe name is called, by entering the alias with which that device has registered.

Who Must do What Before FindMe™ Can Be Used?

FindMe™ is an optional feature on the VCS, and you must install the appropriate option key before it can be used. Contact your TANDBERG representative for more information.

The following steps are required for the use of FindMe once the option has been installed:

1. The VCS administrator enables and configures User Policy.
2. The VCS administrator creates a user account for each user or group who require a FindMe name.
3. The owner of the FindMe name configures their account settings.

FindMe is supported by clustering. For specific information about how FindMe information is managed across Peers in a cluster, refer to the section Clustering and FindMe.

User Policy Manager

The User Policy Manager is the application that manages the FindMe user accounts.

The VCS has its own local User Policy Manager. However, it also provides the ability to use a User Policy Manager on a remote system; this feature is intended for future third party integration.

FindMe™ (User Policy)

Enabling FindMe on the VCS

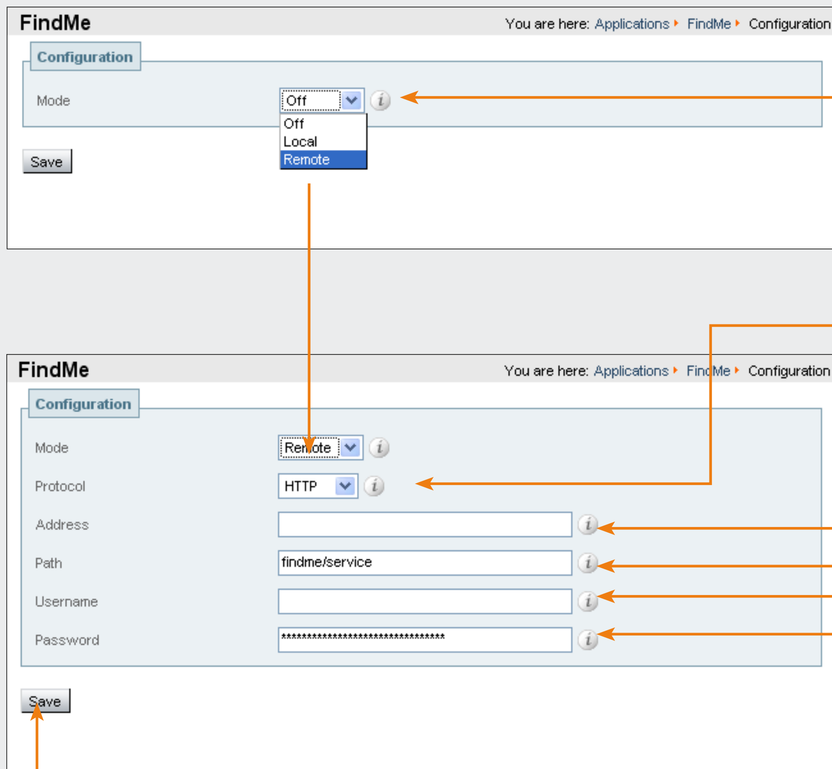
Configuring User Policy Manager

FindMe requires a User Policy Manager. The VCS has its own User Policy Manager, but there is also the ability to connect to a User Policy Manager located on another system.

To configure the User Policy Manager:

- Applications > FindMe > Configuration.
  You will be taken to the User Policy page.
- `xConfiguration Policy UserPolicy`

Administrator Policy will always be applied regardless of the User Policy mode.



Mode

Determines whether or not User Policy will be enabled, and if so, the location of the User Policy Manager.

Off: User Policy is not enabled.

Local: User Policy is enabled and the VCS's own User Policy Manager is used.

Remote: User Policy is enabled and a third-party User Policy Manager located on another system is used (this feature is intended for future third-party integration). If you select this option, further configuration options will appear (see below).

Protocol

The protocol used to connect to the remote User Policy Manager.

Address

The IP address or domain name of the remote User Policy Manager.

Path

The URL of the remote User Policy Manager.

Username

The username used by the VCS to log in and query the remote User Policy Manager.

Password

The password used by the VCS to log in and query the remote User Policy Manager.

Save

Click here to save your changes.

Managing FindMe User Accounts

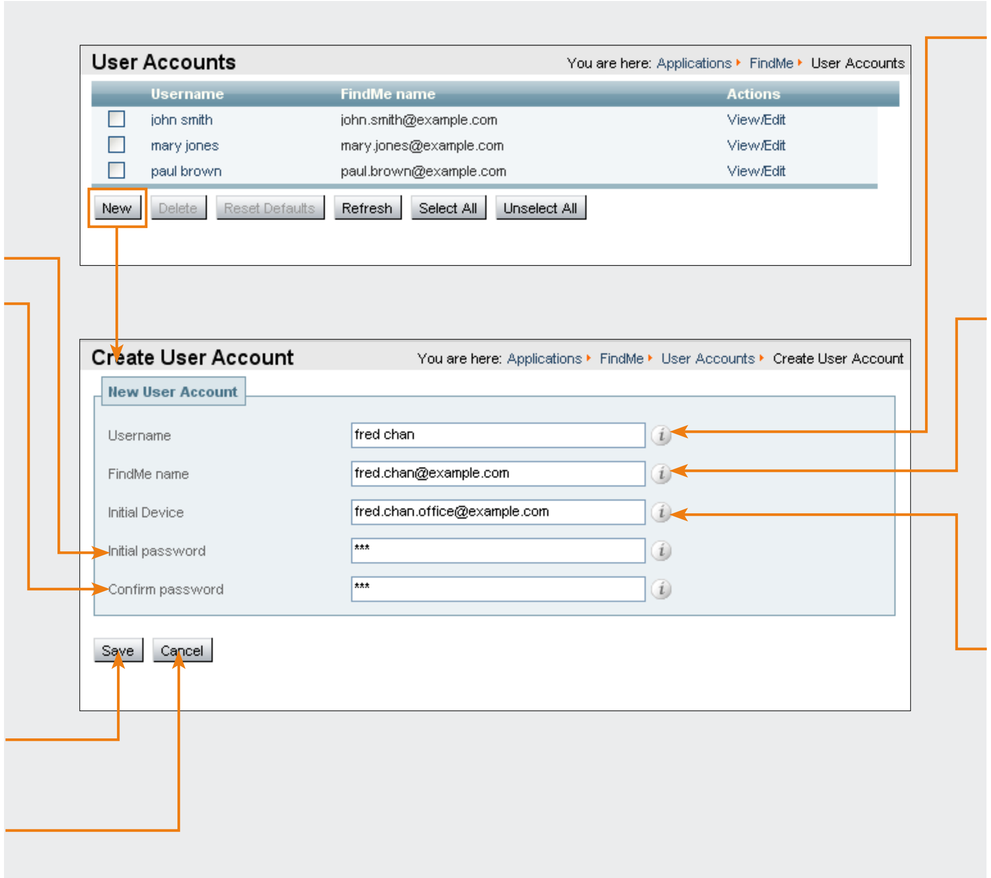
About User Accounts

FindMe user accounts must be created by the VCS Administrator before they can be accessed and configured by users.

Each user account is accessed via a username and password associated with a specific FindMe name.

Creating a New User Account

- Applications > FindMe > User Accounts.
  You will be taken to the User Accounts page.
  Select New.
  You will be taken to the Create User Account page.



Initial password

The password to be used along with the Username when logging into this account.

Users will be able to change the password for their account once they have logged in.

Confirm password

Retype the password.

Save

Click here to create the new account and return to the User Accounts page.

Cancel

Click here to return to the User Accounts page without creating the new account.

Username

The name of the user for whom you are creating an account. This is the name they will use to log in when configuring their FindMe options.

FindMe name

The FindMe name on which the user can be contacted.

The FindMe name can be any string of up to 60 characters. However, not all endpoints are able to dial aliases with spaces or other non-alphanumeric characters so we recommend that these are not used in your FindMe names.

Initial device

The address or alias of an endpoint on which this user can be contacted initially. Once the account has been saved, the user can add and remove endpoints themselves.

FindMe™ (User Policy)

Managing FindMe User Accounts

Changing a User Password

You can change a password on behalf of a user without knowing their existing password. This is useful when the user has forgotten their password.

To change the password:

- VCS Configuration > Policy > User Accounts.
  You will be taken to the User Accounts page.
  Click on the user account whose password you wish to change.
  You will be taken to the Edit User Account page.

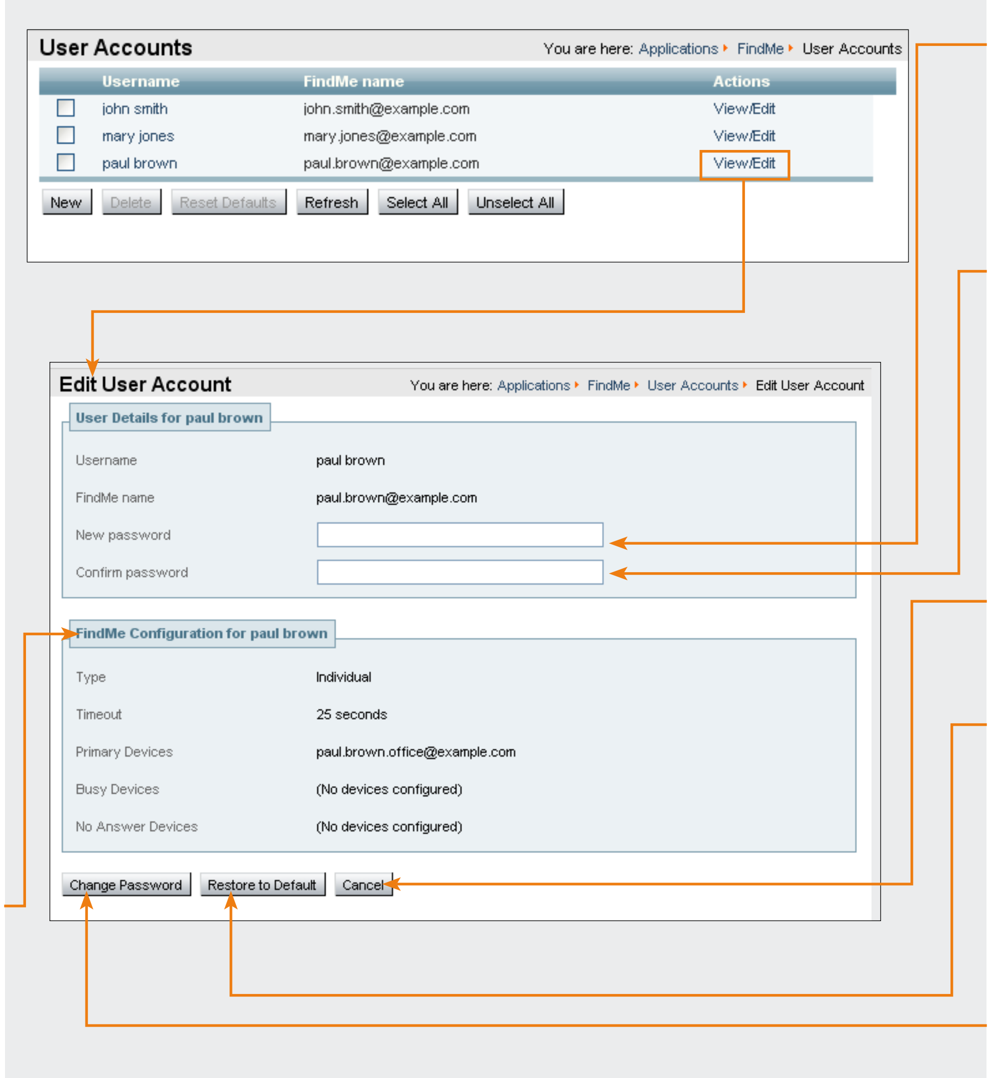
Viewing Existing User Account Settings

To view the configuration of an existing user account:

- VCS Configuration > Policy > User Accounts.
  You will be taken to the User Accounts page.
  Click on the user account whose password you wish to change.
  You will be taken to the Edit User Account page.

FindMe Configuration for...

This section shows you the current configuration for the user.



New password

Type the new password to be used along with the Username when logging into this account.

Confirm password

Retype the new password.

Cancel

Click here to return to the User Accounts page without changing the password.

Restore to Default

Click here to delete any existing configuration for this FindMe name. This will have the effect that any calls to that FindMe name will be rejected until one or more devices are reconfigured for that account.

Change Password

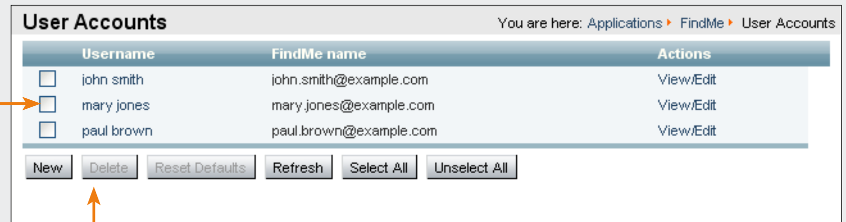
Click here to update the password and return to the User Accounts page.

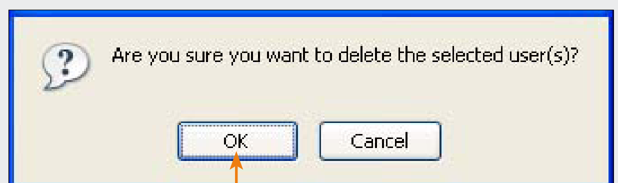
Managing FindMe User Accounts

Deleting a User Account

To delete a FindMe user account:

- VCS Configuration > Policy > User Accounts.
  You will be taken to the User Accounts page.





Tick the box next to the account you wish to delete.

To select all the accounts, click on Select All.

Delete

Click here to delete the selected accounts.

Are you sure...?

A confirmation window will appear to ensure that you wish to proceed. Click OK to continue.

About your FindMe User Account

About FindMe™

The FindMe feature allows you as an individual or part of a group to have a single name on which you can always be called, and you chose where calls to that name will be routed. You can also determine what happens if your first choices are either busy or unanswered after a certain period of time.

For example, you could set up your individual FindMe name so that it will call you on your desktop endpoint first. If there's no answer after 10 seconds it will divert the call to your mobile phone, and if your desktop phone is busy it will divert the call to your colleague's desktop videophone.

Alternatively, you could have a single FindMe name for your team, and set it up so that all the team member's desktop videophones will ring when anyone calls the FindMe name.

FindMe User Accounts

Each FindMe name has an associated user account. Your FindMe user account is set up by your system administrator. Once this has been done, you can log in to your account via a web interface and configure it with details of the device(s) on which you want to be contacted:

- when a call is first placed to your FindMe name
- if any or all of your first choice of devices are busy
- if all of your first choice of devices are unanswered

You can update these details as often as you wish.

Individual versus Group FindMe

There are two types of FindMe names: individual and group.

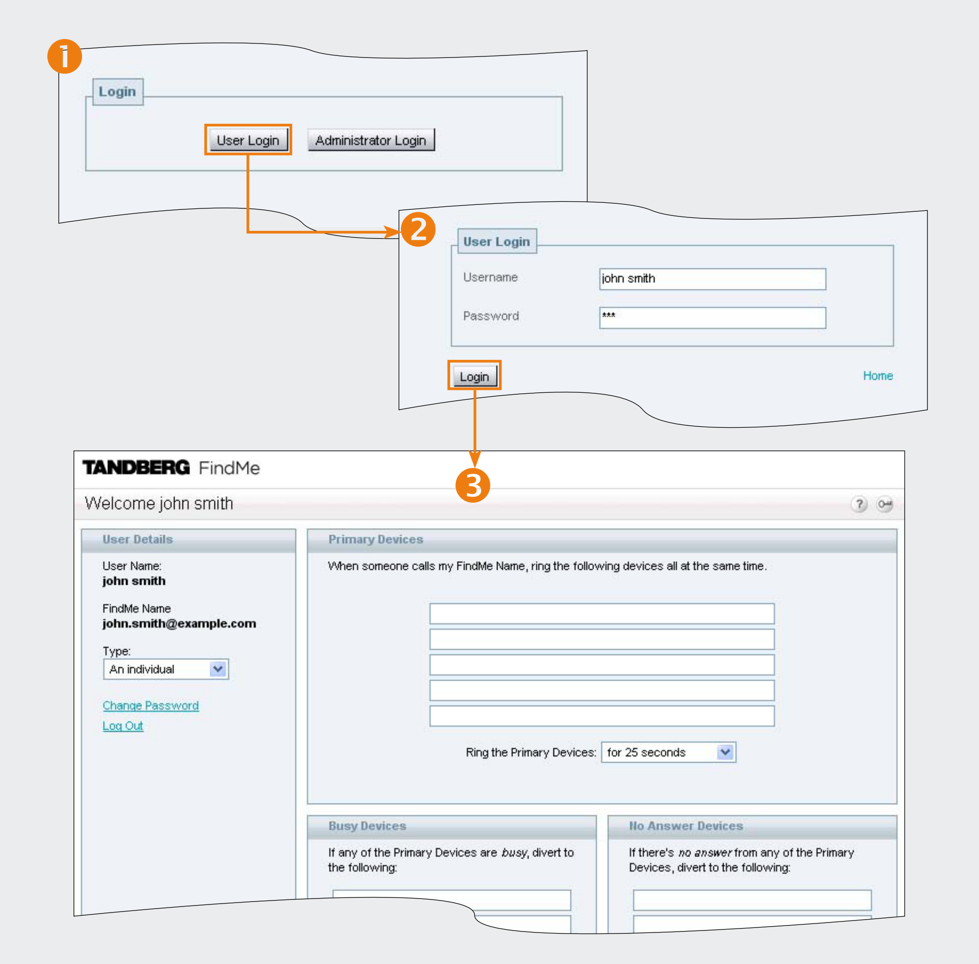
The only difference between the two is what happens if one of the devices in the initial list is busy.

For *individuals*, it is assumed that you will only be able to take calls on one device at a time, therefore if *any* devices in your Primary list are busy, the call will immediately divert to the device(s) in your Busy list.

For *groups*, it is assumed that more than one person is available to take calls, so the call will only divert to the device(s) in the Busy list if *all* devices in the Primary list are engaged.

Accessing the FindMe Configuration Page

To configure your FindMe user account, log in via a web browser as described below:



1. Go to the FindMe link provided to you by your system administrator.

   This will take you to the Login page.

   Select User Login.

2. Enter the Username and Password provided to you by your System Administrator.

   Select Login.

3. You will be taken to the FindMe page. From here you can configure your FindMe options as either an individual or a group.

Configuring your FindMe User Account

If no devices are configured for a FindMe name, all calls to that name will be rejected.

Username

The username for this FindMe account.

FindMe name

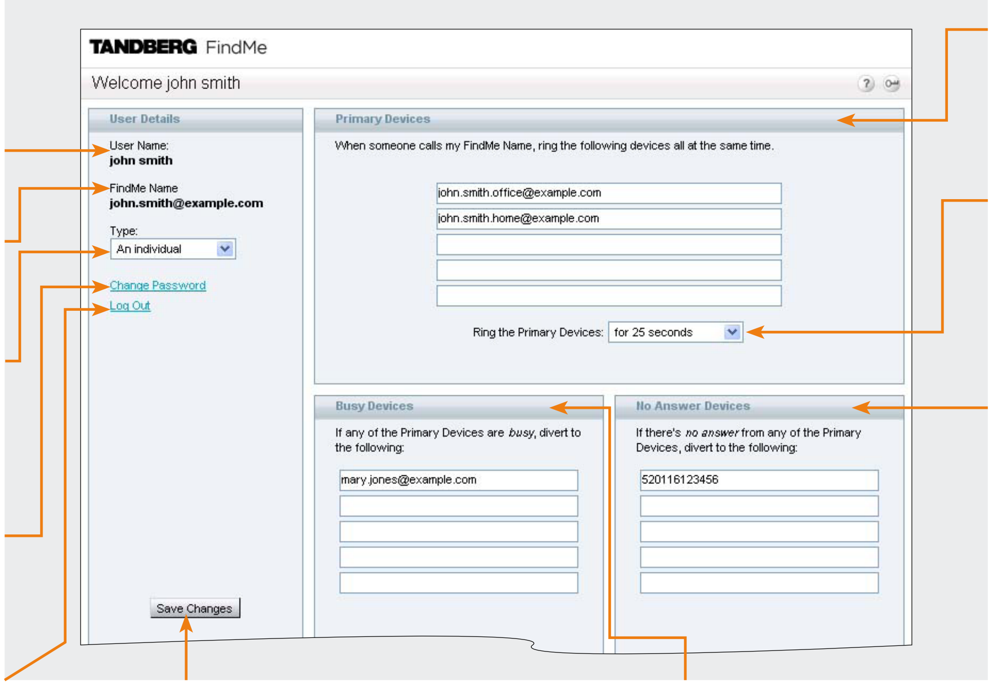
The FindMe name being configured.

Type

Select whether this FindMe name is to apply to an individual or a group of people. This will affect how calls are diverted to the Busy devices.

Change Password

Click here to change the password used to access your FindMe account. You will be taken to a new page where you can enter the new password.



Primary Devices

List the all the device(s) that will ring when your FindMe name is first dialed.

If more than one device is listed here, they will all ring at the same time.

Ring the primary devices

Select the amount of time in seconds you wish the devices in the Primary list to ring before the call is diverted. Alternatively, you can specify that the devices will ring until the caller hangs up.

No Answer Devices

List all the device(s) that will ring if none of the devices in the Primary list are answered within the specified time.

If no devices are listed here, the caller will receive a "no answer" response if none of the Primary devices are answered.

If you have selected a Timeout period of ring until caller hangs up, you will not be able to list any devices here.

Log Out

Click here to exit the FindMe page.

Save Changes

Click here to update your FindMe account with any changes.

Busy Devices

For an individual, list all the device(s) that will ring immediately if *any* of the devices in the Primary list are busy.

For a group of people, list all the device(s) that will ring immediately if *all* of the devices in the Primary list are busy. (If *some* of the devices in the Primary list are busy, the rest will continue to ring for the specified time before the call will divert to the devices listed here.)

If no devices are listed in this section, the caller will get a busy response if any/all of the Primary devices are busy.

Ensure that none of the Primary devices are set to Autoanswer. If they are, the system will consider the call to have been answered when Autoanswer is initiated, and so it will not divert the call to any other devices.

Adding a device to a list

You can have up to five devices in each list. To add a device to any of the lists, enter one of the following in any of the available fields:

- for video endpoints: enter any alias with which the device is registered.
- for 3G mobile phones: to route video to your mobile phone, you must have a 3G gateway - enter the gateway's prefix followed by the mobile phone number. To route voice only, enter the mobile phone number along with any prefixes required by your dial plan for external calls.
- for telephones: enter the extension number (for internal calls) or telephone number, along with any necessary prefixes.

Removing a device

To remove a device from a list, delete it from the relevant field and click Save Changes.

Presence

Overview

Presence is the ability of endpoints to provide information to other users about their current status - such as whether they are offline, online, or in a call. Any entity which provides presence information, or about whom presence information can be requested, is known as a presentity. Presentities publish information about their own presence status, and also subscribe to the information being published by other presentities and FindMe users.

Endpoints that support presence, such as the next release of TANDBERG Movi, can publish their own status information. The VCS can also provide basic presence information on behalf of endpoints that do not support presence, including H.323 endpoints, as long as they have registered with an alias in the form of a URI.

If FindMe is enabled, the VCS can also provide presence information about FindMe users by aggregating the information provided by each presentity configured for that FindMe user.

The Presence application on the VCS supports the SIP-based SIMPLE standard and is made up of two separate services. These are the Presence Server and the Presence User Agent (PUA). These services can be enabled and disabled separately.

The Presence status pages provide information about the presentities who are providing presence information and the users who are requesting presence information on others.

Presence is supported by clustering. For specific information about how Presence information is managed across Peers in a cluster, refer to the section Clustering and Presence.

Presence Server

The Presence Server application on the VCS is responsible for managing the presence information for all presentities in the SIP domain(s) for which the VCS is authoritative (refer to the Configuring SIP - Domains section for more information). The Presence Server can manage the presence information for locally registered endpoints and presentities whose information has been received via a SIP Proxy (e.g. another VCS Control or Expressway).

The Presence Server is made up of the following services, all of which are enabled (or disabled) simultaneously when the Presence Server is enabled (or disabled):

- Publication Manager - receives PUBLISH messages, which contain the status information about a presentity, and writes this information to the Presence Database. PUBLISH messages are generated by presence-enabled endpoints and by the Presence User Agent (PUA).
- Subscription Manager - handles SUBSCRIBE messages, which request information about the status of a presentity. Upon receipt of a SUBSCRIBE message, the Subscription Manager sends a request to the Presentity Manager for information about that presentity, and forwards the information that is returned to the subscriber. The Subscription Manager also receives notifications from the Presentity Manager when a presentity's status has changed, and send this information to all subscribers.
- Presentity Manager - an interface to the Presence Database. It is used to support VCS features such as FindMe and the PUA, where the presence information provided by a number of different devices must be aggregated in order to provide an overall presence status for one particular presentity.
  When the Presentity Manager receives a request from the subscription manager for information on a presentity, it queries the Presence Database for all information available on all the endpoints associated with that particular presentity. The Presentity Manager then aggregates this information to determine the presentity's current status, and returns this to the Subscription Manager.
- Presence database - stores current presence information received in the form of PUBLISH messages. Also sends NOTIFY messages to the Presentity Manager to inform it of any changes.

Presence User Agent (PUA)

Overview

Endpoints that do not support presence, including all H.323 endpoints, can have status published on their behalf by the VCS. The service that publishes this information is called the Presence User Agent (PUA).

The PUA takes information from the local registration database and the call manager and determines, for each endpoint that is currently locally registered, whether or not it is currently in a call. The PUA then provides this status information via a PUBLISH message.

In order for the PUA to successfully provide presence information about a locally registered endpoint:

- the endpoint must be registered with an alias in the form of a URI
- the domain part of the URI must be able to be routed to a SIP Registrar that has a presence server enabled. (This could be either the local Presence Server, if enabled, or another Presence Server on a remote system.)

When enabled, the PUA generates presence information for all endpoints registered to the VCS, including those which already support presence. The status information provided by the PUA is either:

- online (registered but not in a call)
- in call (registered and currently in a call).

Aggregation of Presence Information

When enabled, the PUA generates presence information for all endpoints registered to the VCS, including those which already support presence. However, endpoints that support presence may provide other, more detailed status, for example away or do not disturb. For this reason, information provided by the PUA is used by the Presentity Manager as follows:

- Where presence information is provided by the PUA and one other source, the non-PUA presence information will always be used in preference to the PUA presence information. This is because it is assumed that the other source of information is the presentity itself, and this information is more accurate.
- Where presence information is provided by the PUA and two or more other sources, the Presence Server will aggregate the presence information from all presentities to give the 'highest interest' information, e.g. online rather than offline, and in call rather than away.
- If no information is being published about an endpoint, either by the endpoint itself or by the PUA, the endpoint's status will be offline. If the PUA is enabled, the offline status indicates that the endpoint is not currently registered.

FindMe presence

When the Presentity Manager receives a request for information about the presences of a FindMe alias, it looks up the presence information for each endpoint that makes up that FindMe alias. It then aggregates this information as follows:

- if the FindMe alias is set to Individual mode, if any one of the endpoints making up that FindMe is in a call the FindMe presentity's status will be reported as in call.
- if the FindMe alias is set to Group mode, if any one of the endpoints is online (i.e. not in call or offline) then the FindMe presentity's status will be reported as online.

Registration refresh period

The PUA will update and publish presence information on receipt of:

- a registration request (for new registrations)
- a registration refresh (for existing registrations)
- a deregistration request
- call setup and cleardown information.

For non-traversal H.323 registrations the default registration refresh period is 30 minutes. This means that when the PUA is enabled on a VCS with existing registrations, it may take up to 30 minutes before an H.323 registration refresh is received and available presence information is published for that endpoint.
It also means that if an H.323 endpoint becomes unavailable without sending a deregistration message, it may take up to 30 minutes for its status to change to offline. To ensure more timely publication of presence information for H.323 endpoints, you should decrease the H.323 registration refresh period (via VCS Configuration > Protocols > H.323 > Gatekeeper > Time to live).

The default registration refresh period for SIP is 60 seconds, so it will take no more than a minute for the PUA to publish updated presence information on behalf of any SIP endpoints.

Enabling and Disabling Presence Services

Presence Services (i.e. the Presence Server and the Presence User Agent) are both disabled by default.

These services can be enabled and disabled separately from each other, depending on the nature of your deployment.

PUA

Enabled

If the PUA is enabled, it will publish presence information for all locally registered endpoints, whether or not those endpoints are also publishing their own presence information. Information published by the PUA will be routed to a Presence Server acting for the endpoint's domain. This could be the local Presence Server, or (if this is disabled) a Presence Server on another system that is authoritative for that domain.

Disabled

If the PUA is disabled, only those endpoints that support presence will publish presence information. No information will be available for endpoints that do not support presence.

The recommended configuration for a VCS Expressway when acting as a traversal server for a VCS Control is to enable the PUA and disable the Presence Server on the VCS Expressway, and enable the Presence Server on the VCS Control. This will ensure that all PUBLISH messages generated by the PUA are routed to the VCS Control.

Presence Server

Regardless of whether or not the Presence Server is enabled, the VCS will still continue to receive PUBLISH messages if they are sent to it from any of the following sources:

- locally registered endpoints that support presence
- the local PUA (if enabled)
- remote SIP Proxies

Enabled

If the local Presence Server is enabled, it will process any PUBLISH messages intended for the SIP domains for which the local VCS is authoritative. All other PUBLISH messages will be proxied on in accordance with the VCS's SIP routing rules.

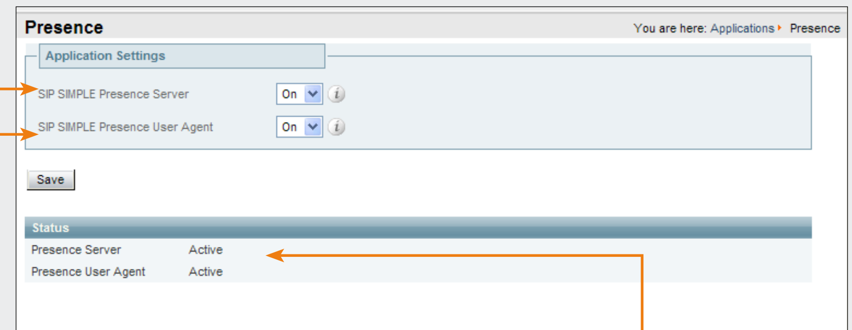
Disabled

If the local Presence Server is disabled, the VCS will proxy on all PUBLISH messages to one or more of its neighbor zones in accordance with its locally configured call processing rules. The local VCS will do this regardless of whether or not it is authoritative for the presentity's domain. If one of these neighbors is authoritative for the domain, and has a Presence Server enabled, then that neighbor will provide presence information for the presentity.

We recommend that if you have a deployment with two or more VCSs neighbored together, you enable the presence server on just one VCS. This will ensure a central source of information for all presentities in your network.

To enable and disable the Presence Server and Presence User Agent:

- Applications > Presence
  You will be taken to the Presence page.
- xConfiguration Applications Presence



SIP SIMPLE Presence Server

Enables or disables the Presence Server.

SIP SIMPLE Presence User Agent

Enables or disables the Presence User Agent.

Status

This section shows whether the Presence Server and Presence User Agent are active or inactive.

For information about how Presence works within a VCS cluster, see the Clustering and Presence section.

Viewing Presence Status

Publishers

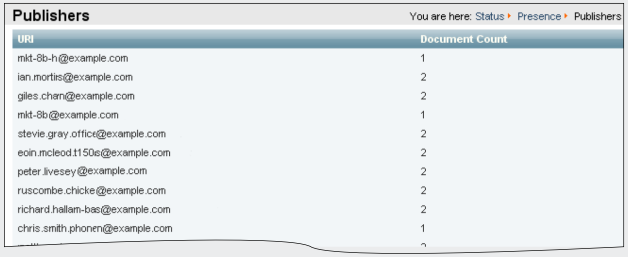
Status > Presence > Publishers

This page lists each Presentity whose presence information is being managed by (i.e. published to) the local Presence Server. All Presentities are listed here regardless of whether or not anyone is requesting their presence information. If there are no Publishers listed, this could mean that the Presence Server is not enabled on this VCS.

Note: FindMe users are not listed here as they do not have their status individually published. The status of a FindMe user is based on the published status of the endpoints and/or presentities that make up the FindMe user, and is determined by the Presentity Manager.

Document Count: The number of sources of information that are being published for this particular presentity. All endpoints that are registered to the VCS will have information published on their behalf by the PUA (as long as they are registered with an alias in the form of a URI). If an endpoint supports presence, it may also publish its own presence information. This means that some presentities will have more than one source of information about their presence. It is the job of the Presentity Manager to aggregate this information and determine the actual status of the presentity.

URI: The address of the presentity whose presence information is being published.



Presentities

Status > Presence > Presentities

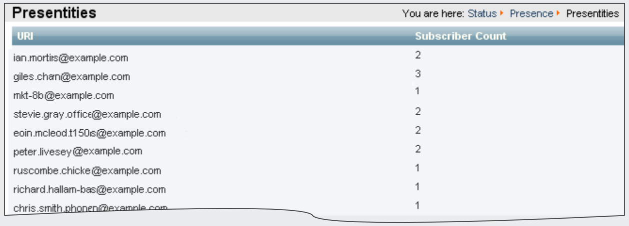
This page lists each presentity whose presence information is being managed by (i.e. published to) the local Presence Server and whose presence information has been requested by a subscriber. Presentities are listed here whether or not there is any information currently available about that presentity. If a presentity has been subscribed to but there is no information being published about it, then it will be listed here if the local presence server is authoritative for the presentity's domain. Presentities are listed here regardless of whether the subscriber that requested the information is registered locally or to a remote system.

Note: FindMe users will be listed here if their presence information has been requested by a subscriber.

URI: The address of the presentity whose presence information has been requested.

Subscriber Count: The number of endpoints who have requested information about that particular presentity.

To view the list of all subscribers who are requesting information about a particular presentity, click on the presentity's URI.



Subscribers

Status > Presence > Subscribers

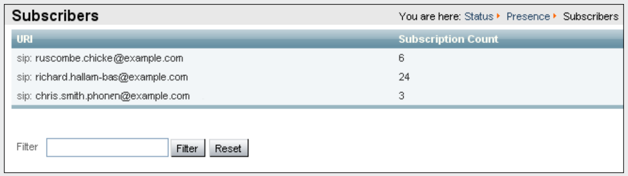
This page lists each endpoint that has requested information about one or more presentities whose information is managed by (i.e. published to) the local presence server. Endpoints requesting this information are listed here regardless of whether they are registered locally or to a remote server.

Note: FindMe users will not be listed here as a FindMe entity cannot subscribe to presence information. However, one or more of the endpoints that make up a FindMe user may be requesting presence information, in which case that endpoint will be listed here.

URI: The address of the endpoint that has requested presence information.

Subscription Count: The number of local presentities about whom this endpoint is requesting information.

To view the list of all local presentities whose information is being requested by a particular endpoint, click on the endpoint's URI.



Maintenance

This section describes the pages that appear under the Maintenance menu of the VCS web interface.

These pages allow you to perform the following tasks:

- upgrade to a new release of software
- downgrade to a previous version of software
- install and delete Option Keys
- manage security certificates
- manage Administrator accounts and passwords
- create a system snapshot
- restart the VCS
- shut down the VCS

This section also gives information on:

- restoring the system to its default settings
- password encryption.



Upgrading Software

Overview

It is possible to install new releases of the VCS software on your existing hardware. Software upgrade can be done via the VCS in one of two ways:

- using secure copy (SCP/PSCP)
- using the web interface (HTTP/HTTPS).

This section describes how both of these methods are used to perform upgrades.

You can also upgrade the VCS software via TMS. See the TMS guide for more information.

Prerequisites

The upgrade requires you to have:

- a valid Release key. This is required for upgrades to a major release, e.g. X2.1 to X3.0; it is not required for dot releases, e.g. X3.0 to X3.1)
- a software image file.

Contact your TANDBERG representative for more information on how to obtain these.

Backing up current configuration

The VCS's existing configuration will be restored after performing an upgrade. However, we recommend that you make a backup of the configuration before upgrading. How you do this will depend on the version of software currently running.

Versions prior to X3..0

1. Use the command line interface to log on to the VCS.
2. Issue the command `xConfiguration`.
3. Save the resulting output to a file, using cut-and-paste or some other means provided by your terminal emulator.

To restore your configuration:

1. Remove the `*c` from in front of each command.
2. Paste this information back in to the command line interface.

Version X3.0 and above

Backups can be made automatically. See the Backup and Restore section for full details.

Upgrading and Option Keys

All existing option keys will be retained through the upgrade from one version of software to the next, including upgrades to the next major release. However, we recommend that you take note of your existing option keys before performing the upgrade.

New features may also become available with each major release of VCS software, and you may need to install new option keys if you wish to take advantage of these new features. Contact your TANDBERG representative for more information on all the options available for the latest release of VCS software.

Installing and Restarting

Upgrading software is a two-stage process. Firstly, the new software image is uploaded onto the VCS. At the same time, the current configuration of the system is recorded, so that this can be restored after the upgrade. During this initial stage the system will continue running on its existing software version, and all normal system processes will continue.

The second part of the upgrade involves restarting the system. It is only during the restart that the VCS installs the new software version and restores the previous configuration.

This means that you can upload the new software to your system at any time, and then wait until a convenient moment (for example, when no calls are taking place) to install the new version by rebooting the system. However, this also means that any configuration changes made between the upload and the reboot will be lost once the system restarts using the new software version.

For security reasons we recommend that you change the admin password after upgrading to X3.0.

For specific information about upgrading and downgrading for Peers in a cluster, refer to the Upgrades and Downgrades section of the clustering chapter.

Upgrading Using SCP/PSCP

To upgrade using SCP or PSCP (part of the PuTTY free Telnet/SSH package) you will need to transfer two files to the VCS:

- a text file containing just the 16-character Release Key (not required for dot release upgrades). Ensure there is no extraneous white space in this file.
- the file containing the software image.

Once these files have been transferred:

1. Ensure the VCS is turned on and available over IP.
2. Upload the release key file using SCP/PSCP to the `/tmp` folder on the system. The target name must be `release-key`, e.g.

   `scp release-key root@10.0.0.1:/tmp/release-key`
   or
   `pscp release-key root@10.0.0.1:/tmp/release-key`
3. Enter the admin password when prompted.
4. Upload the software image using SCP/PSCP to the `/tmp` folder on the system. The target name must be `/tmp/tandberg-image.tar.gz`, e.g.

   `scp s42100x30.tar.gz root@10.0.0.1:/tmp/tandberg-image.tar.gz` or
   `pscp s42100x30.tar.gz root@10.0.0.1:/tmp/tandberg-image.tar.gz`
5. Enter the admin password when prompted.
6. Wait until the software has installed completely. This should not take more than five minutes.
7. Log in again and reboot the system.

After about five minutes the system will be ready to use.

You must name the files exactly as described above.

You must transfer the Release Key file before transferring the software image.

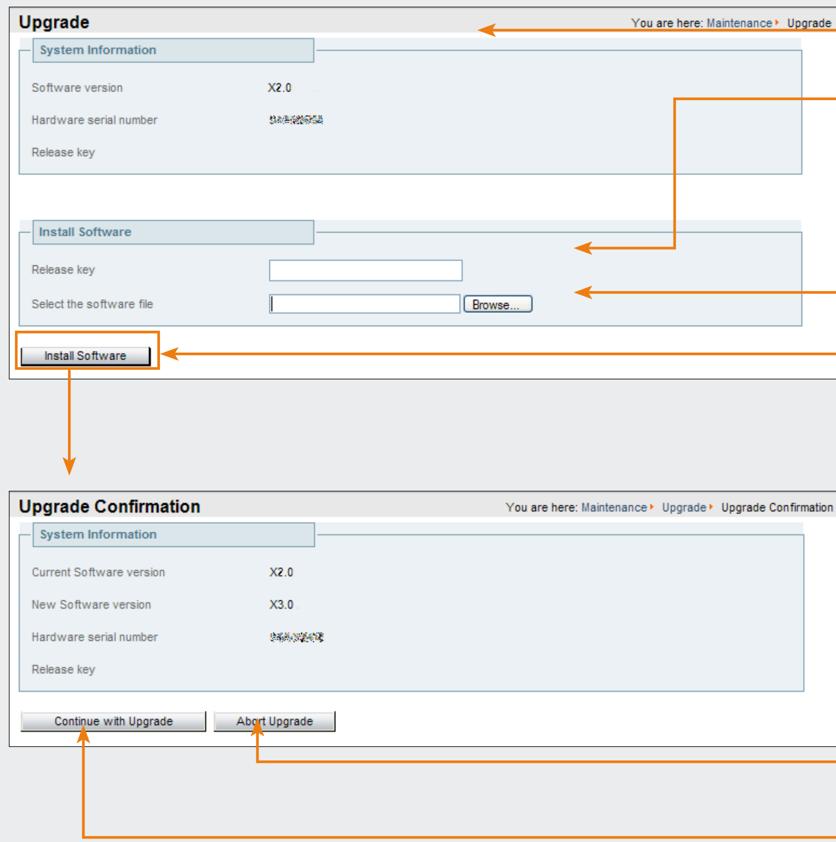
Upgrading via the Web Interface

To upgrade your software via the web interface:

- Maintenance > Upgrade.
  You will be taken to the Upgrade page.

You must restart the system after you have uploaded the new software version and confirmed the upgrade, in order for the installation to complete. Any configuration changes you make between confirming the upgrade and restarting will be lost, so we recommend restarting your system immediately.

Before you start the upgrade, ensure that the software image file for the new version has been saved in a network location that can be accessed via the web interface. Also ensure that you have the 16-character Release Key readily available (this is not required if you are upgrading to a dot release, e.g. X3.0 to X3.1).



System Information

This section tells you about the software and hardware that currently make up your system.

Release key

Enter the 16-character Release Key that has been provided to you. This is not required if you are upgrading to a dot release, e.g. X3.0 to X3.1.

If you have cut and pasted the release key, ensure there are no leading or trailing spaces.

Select the software file

Enter the path of the software image file, or click Browse to locate it on the network.

Install Software

Click Install Software. After a few moments you will be taken to the Upgrade Confirmation page. This page will list any warnings of which you need to take note before proceeding with the upgrade.

Abort Upgrade

Click here to cancel the upgrade and return to the Upgrade page.

Continue with Upgrade

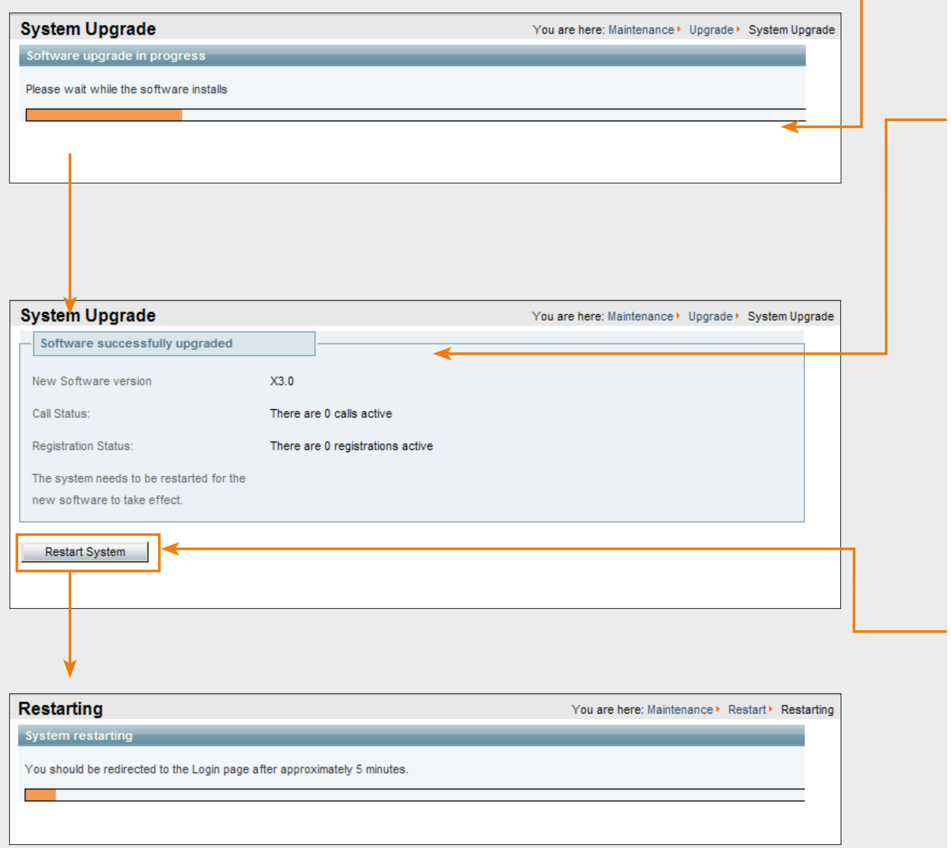
Check the details and click Continue with Upgrade to proceed.

Upgrading via the Web Interface (cont.)

(Continued from previous page)

You must restart the system after you have uploaded the new software version and confirmed the upgrade, in order for the installation to complete. Any configuration changes you make between confirming the upgrade and restarting will be lost, so we recommend restarting your system immediately.

Before you start the upgrade, ensure that the software image file for the new version has been saved in a network location that can be accessed via the web interface. Also ensure that you have the 16-character Release Key readily available (this is not required if you are upgrading to a dot release, e.g. X3.0 to X3.1).



Software upgrade in progress

This screen appears while the new version of software is being copied to your system.

Software successfully upgraded

This screen indicates that the software has been copied to your system successfully.

You will need to restart the VCS in order for the new version to take effect. Restarting will cause all current calls to terminate, and all current registrations to be ended. This page indicates the number of active calls and registrations on your VCS so that you can restart it at an appropriate time.

If you do not restart the system immediately, you should refresh this page before restarting to check the current status of calls and registrations.

Restart system

Click here after checking the active calls and registrations to ensure that it is an appropriate time to restart the VCS.

The system will restart and after a few minutes you will be taken to the Login screen.

The upgrade is now complete.

Downgrading Software

Downgrade Procedure

The procedure for downgrading software is essentially the same for upgrading software, except for the software image being used.

Prerequisites

The downgrade requires you to have:

- a valid Release key.
- a software image file.

You should already have obtained these when the previous version of the software was installed on your VCS.

Backing up current configuration

The VCS's existing configuration will be restored after performing a downgrade, with the exception of those configuration items relating to new features introduced in X3.0.

However, we recommend that you make a backup of the configuration before downgrading. Version X3.0 has an automated backup feature, but note that this will only allow you to restore the backed up configuration to a VCS running X3.0. See the Backup and Restore section for full details.

Impact on features introduced in X3.0

VCS software version X3.0 introduces a number of new features. Should you install this version and then subsequently downgrade to a previous version of the VCS software you must note the following.

Encrypted Passwords

Any passwords that existed prior to upgrading to X3.0, and any that were subsequently created, will be deleted upon downgrade from version X3.0. The password for the default admin administration account will revert to the default of TANDBERG.

Additional Administration accounts

If you have created one or more Administration Accounts, these will all be deleted upon downgrading from version X3.0.

Clustering

After downgrading from X3.0, Peers in a cluster will no longer share information about Bandwidth, Presence, and FindMe. They will revert to treating each other as Alternates.

Presence Services

Presence will no longer be supported after downgrading from version X3.0.

Local Zone Matches

Any local zone matches will be deleted after downgrading from version X3.0.

Call Tags

Call tags will not be added or recognized by VCS software prior to X3.0. Once you downgrade from X3.0, any call tags received from other VCSs will be deleted and not forwarded on.

Logging Levels

If you have event logging set to Level 4, after downgrading from X3.0 the Log Level will be set to Level 3.

Option Keys

Overview

Your VCS may have been shipped with one or more optional features pre-installed. Additional VCS features can be added to your existing system by the installation of Option Keys.

To view the list of options installed currently, go to Maintenance > Option Keys. You will be taken to the Option Keys page.

The options that you may see here include:

- Expressway: enables the VCS to work as an Expressway™ firewall traversal server
- H.323 to SIP Interworking gateway: enables H.323 calls to be translated to SIP and vice versa
- User Policy: enables TANDBERG FindMe functionality
- Dual Network Interfaces: enables the LAN 2 port
- Traversal calls: determines the number of traversal calls allowed on the VCS at any one time. A traversal call is any call where the VCS is required to take the media as well as the signalling, i.e. firewall traversal calls, calls that are interworked between IPv4 and IPv6 calls, and calls that are interworked between SIP and H.323. Note that traversal calls that are passing through the VCS from one neighbor to another but where neither endpoint in the call is locally registered will still be counted as one non-traversal call.
- Non-traversal calls: determines the number of non-traversal calls allowed on the VCS at any one time. A non-traversal call is any call where the VCS is taking the signalling but not the media. Note that non-traversal calls that are passing through the VCS from one neighbor to another but where neither endpoint in the call is locally registered will still be counted as one non-traversal call.
- Registrations: the number of concurrent registrations allowed on the VCS. An endpoint can register with more than one alias and this will be considered to be a single registration. However, an endpoint that supports both SIP and H.323 and registers using both protocols will count as two registrations. H.323 systems such as gateways, MCUs and Content Servers can also register with a VCS, and these will each count as one registration.
- Encryption: indicates that AES encryption is supported by this software build.

Contact your TANDBERG representative for more information on how to purchase any of these additional features.

Once the appropriate Option Key has been purchased, options can be installed in either of two ways:

- via the CLI.
- via the web interface.

This section describes both methods.

Some option keys require that the VCS is restarted before the option key will take effect. In such cases you will receive a warning on the web UI, which will remain in place as a reminder until the system has been restarted. However, you can continue to use and configure the VCS in the meantime.

Adding Options via the CLI

To return the indexes of all the Option Keys that are already installed on your system:

- `xStatus Options`

To add a new Option Key to your system:

- `xConfiguration Option [1..64] Key`

When using the CLI to add an extra option key, you can use any unused option index. If you chose an existing option index, that option will be overwritten and the extra functionality provided by that option key will no longer exist. To see which indexes are currently in use, type `xConfiguration option`.

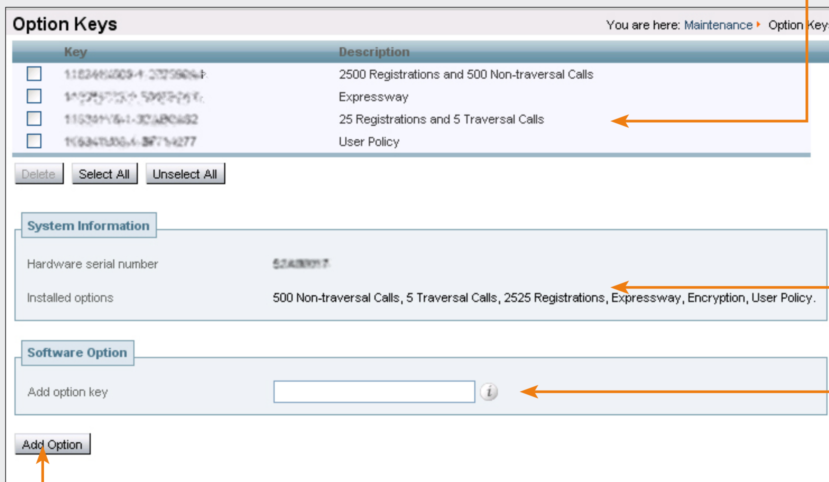
Option Keys

Adding Options via the Web Interface

To add options via the web interface:

- Maintenance > Option Keys.
  You will be taken to the Option Keys page.

Some option keys require that the VCS is restarted before the option key will take effect. You will receive a warning if this is the case.



This section lists the keys that are already installed on your system along with a description of the options they provide.

System Information

This section tells you about the hardware and options that currently make up your system.

Add option key

Enter the 20-character Option Key that has been provided to you for the option you wish to add.

Add Option

Click Add Option.

Overview

For extra security, you may wish to have the VCS communicate with other systems (e.g. servers such as LDAP servers, neighbor VCSs, or clients such as SIP endpoints) using TLS encryption.

For this to work successfully in a connection between a client and server:

- the server must have a certificate installed that verifies its identity. This certificate must be signed by a Certificate Authority (CA).
- the client must trust the CA that signed the certificate used by the server.

The VCS allows you to install appropriate files so that it can act as either a client or a server in connections using TLS.

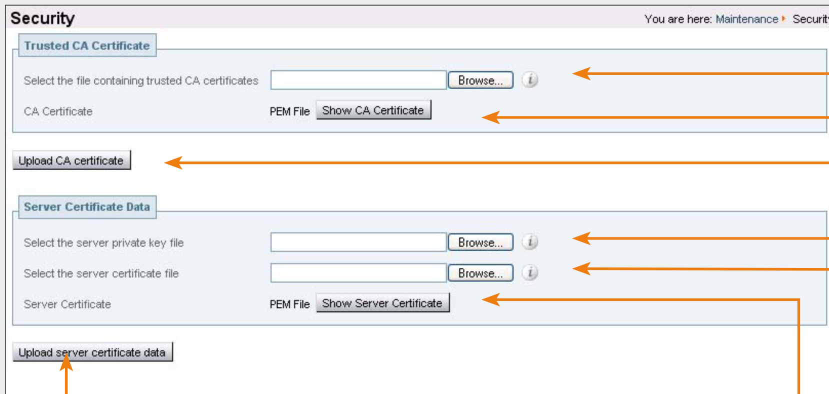
For an endpoint to VCS connection, the VCS will be the TLS server. For a VCS to LDAP server connection, the VCS will be a client. For a VCS to VCS connection either VCS may be the client with the other VCS being the TLS server.

To enable security using the web interface:

- Maintenance > Security.
  You will be taken to the Security page.

The files that enable secure connections over TLS are installed via the web interface. They cannot be installed using the CLI.

Enabling Security



Select the file containing...

Allows you to upload a PEM file that identifies the list of Certificate Authorities trusted by the VCS. The VCS will only accept certificates signed by a CA on this list. If you are connecting to an LDAP database using TLS encryption, the certificate used by the LDAP database must be signed by a CA on this list.

Show CA certificate

Shows you the currently uploaded PEM file that identifies the list of Certificate Authorities trusted by the VCS.

Upload CA certificate

Click here once you have selected the file to upload it.

Select the server private key file

Allows you to upload a PEM file that identifies the private key used to encrypt the server certificate used by the VCS. This private key must not be password protected.

Select the server certificate file

Allows you to upload a PEM file that contains the server certificate used for HTTPS connections to the VCS from user or administrator web browsers, and by SIP endpoints or servers connecting to the VCS over TLS.

Upload server certificate data

Click here once you have selected both the private key and certificate files to upload them.

Show server certificate

Shows you the currently uploaded PEM file containing the certificate used by the VCS to identify itself to SIP and HTTPS clients when communicating over SSL/TLS.

Administration Accounts

Overview

Default Administration Account

The VCS has a default administrator account with full read/write access. This account is used to log into the VCS via the web UI or the CLI. The username for this account is admin (all lower case) and the default password is TANDBERG (all upper case).

You cannot delete the default administrator account or change the admin username, but you should change the password as soon as possible. Choose a strong password, particularly if administration over IP is enabled.

Additional Administration Accounts

You can add up to 15 additional administration accounts with either Read Write access or Read Only access. These can be used to log in via the web UI only.

Administration Access Levels

Read Write

Administration accounts with Read Write access can view and change all configuration available via the web UI. These accounts have exactly the same rights as the default admin user.

Read Only

Administration accounts with Read Only access can view the current status and configuration of the VCS, but cannot make any changes. Some pages, such as the Upgrade page, are blocked to Read Only accounts.

The Configuration Log records all login attempts and configuration changes made via the web UI, and can be used as an audit trail when you have multiple administration accounts.

Adding an Administration Account

See the Supported Characters section for a complete list of characters allowed in these fields.

Name

The username for the administration account. This field is case-senstive.

Password

Enter the password that this administrator will use to log in to the VCS. The password can be up to 16 characters.

All passwords on the VCS are encrypted.

Confirm Password

Retype the password entered above.

Account access

Determines the rights for this account. The options are:

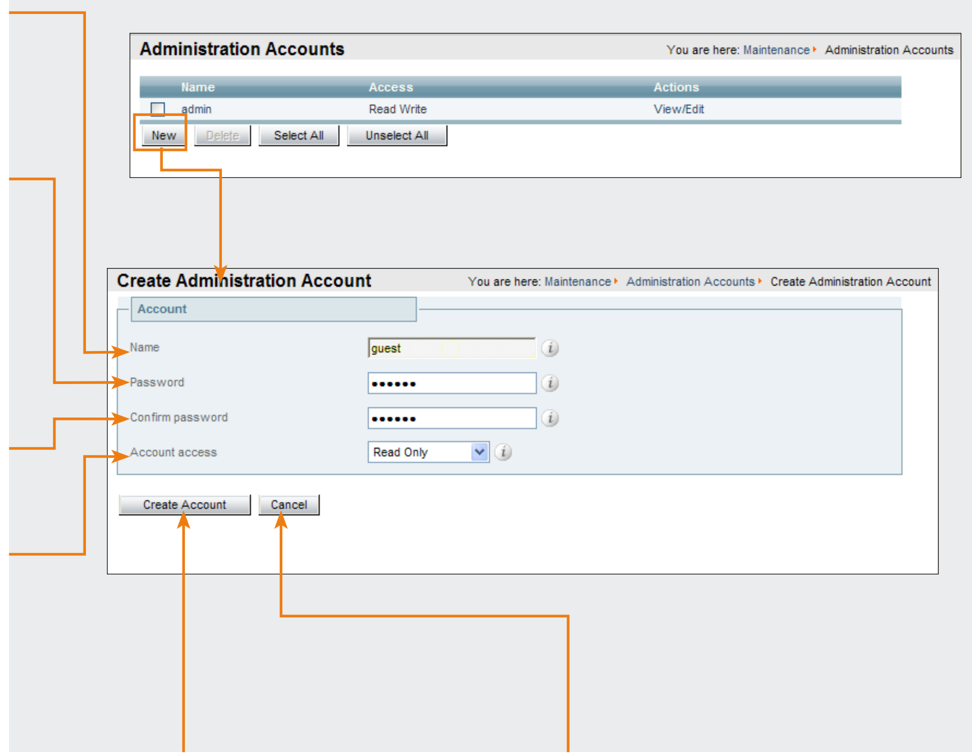
Account Disabled: This account can not be used currently.

Read Only: this account will be able to view but not edit the VCS configuration.

Read Write: this account will have full access to view and edit the VCS configuration.

To add a new Administration account:

- Maintenance > Administration Accounts.
  You will be taken to the Administration Accounts page.
  Click New.
  You will be taken to the Create Administration Account page.



Create Account

Click here to save the account and return to the Administration Accounts page.

Cancel

Click here to return to the Administration Accounts page without creating the account.

Editing an Administration Account

To change the name, password or access level for an existing administration account:

- Maintenance > Administration Accounts.
  You will be taken to the Administration Accounts page.
  Click on the name of the account you wish to edit.
  You will be taken to the Edit Administration Account page.

Name

The username for the administration account. This field is case-senstive.

Password

Enter the password that this administrator will use to log in to the VCS.

The password can be up to 16 characters.

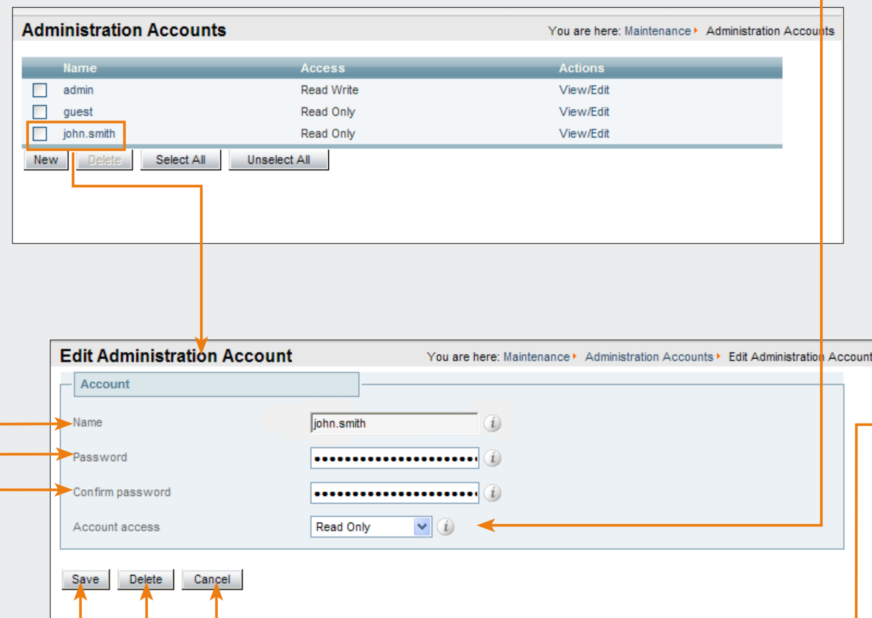
All passwords on the VCS are encrypted, so you will only see placeholder characters here.

Confirm Password

Retype the password entered above.

See the Supported Characters section for a complete list of characters allowed in these fields.

If you forget the password for the admin account, you can still log in as another administration user with Read Write access and change the password for the admin account. If you do not have any other such administration users set up, or you have forgotten those passwords as well, it is possible to reset the password for the admin account as long as you have physical access to the VCS. See the section Resetting the Default Administrator Password for details.



Account access

Determines the rights for this account. The options are:

Account Disabled: This account can not be used.

Read Only: This account will be able to view but not edit the VCS configuration.

Read Write: This account will have full access to view and edit the VCS configuration.

Cancel

Click here to return to the Administration Accounts page without saving your changes.

Delete

Click here to delete this account.

Save

Click here to save the changes to this account.

Backup and Restore

Overview

The Backup and Restore feature allows you to create a file containing the configuration of your VCS at a particular date and time. You can then use this file at a later date to return the VCS to that state of configuration.

We recommend you create a backup in the following situations:

- before performing an upgrade
- before performing a system restore
- in demonstration and test environments if you wish to be able to restore the VCS to a known configuration.

The following settings are included in the backup and restore process:

- all configuration settings
- all FindMe user accounts and settings
- administrator policy
- clustering
- security certificates.

Event logs are not included in the backup.

Limitations

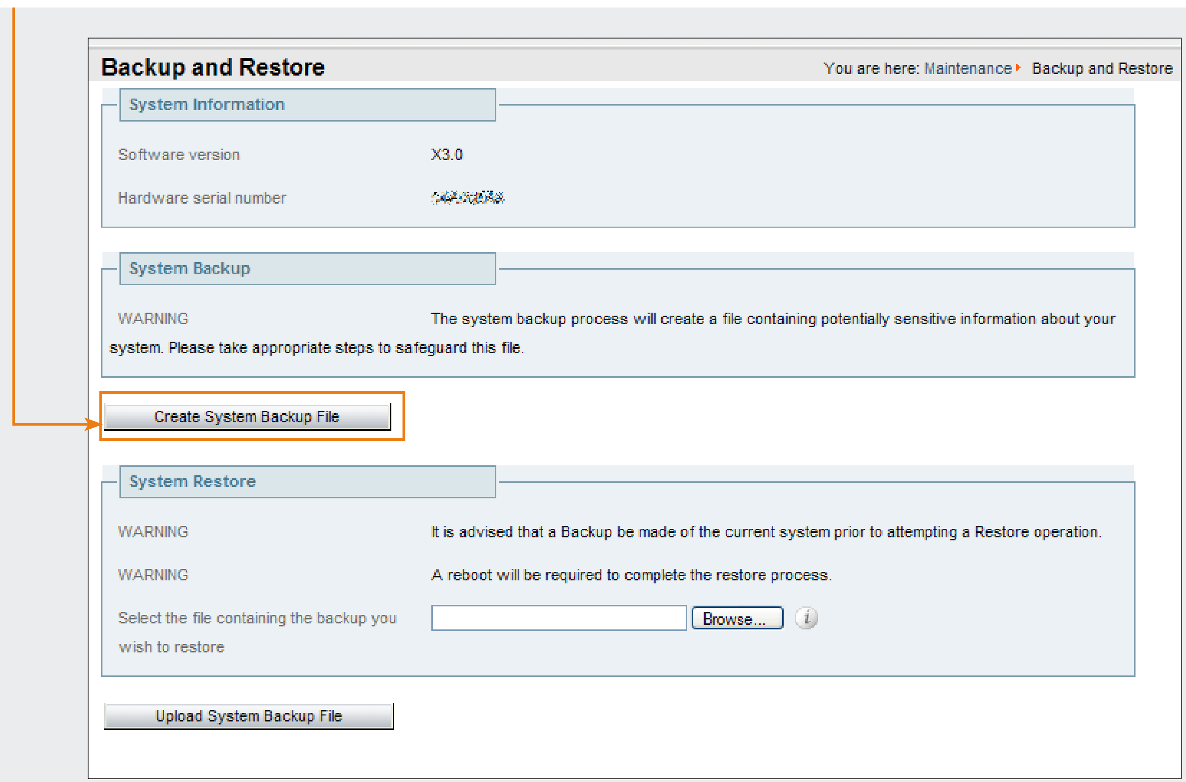
- Backups can only be restored to a VCS running the same version of software from which the backup was made.
- It is possible to create a backup on one VCS and restore it to a different VCS, for example if the original system has failed. However, before performing the restore you must install on the new system the same set of option keys that were installed on the old system. If you do attempt to restore a backup made on a different VCS, you will receive a warning message during the upgrade process, but you will be allowed to continue.
- Backups should not be used to copy configuration between VCSs.

For specific information about backing up and restoring Peers in a cluster, refer to the [Backup and Restore] section of the clustering chapter.

Creating a Backup of your VCS Configuration

To create a backup of the VCS's current configuration:

1. Navigate to Maintenance > Backup and Restore.
   You will be taken to the Backup and Restore page.
2. Click Create System Backup File.
   Once the backup file has been created, a pop-up window will appear giving you the opportunity to save the file (the other options available will depend on your browser). The default name will be in the format `<hardware serial number>_<date>_<time>_backup.tar.gz`.
3. Save the file to a designated location.



Restoring a Previous Backup

To restore the VCS to a previous configuration:

1. Navigate to Maintenance > Backup and Restore.
   You will be taken to the Backup and Restore page.
2. In the System Restore section, Browse to the backup file containing the configuration you wish to restore.
3. Click Upload System Backup File.
   The VCS will check the file and if it is valid, you will be taken to the Restore Configuration page.
   If the backup file is not valid, you will receive an error message at the top of the Backup and Restore page.

The Restore configuration page will show you the current software version and the number of calls and registrations. Continuing with the restore process will cause the VCS to reboot and terminate all calls, so use this page to ensure that there are no calls currently in progress.

Warnings

Read all the warnings that appear in this section before proceeding with the restore.

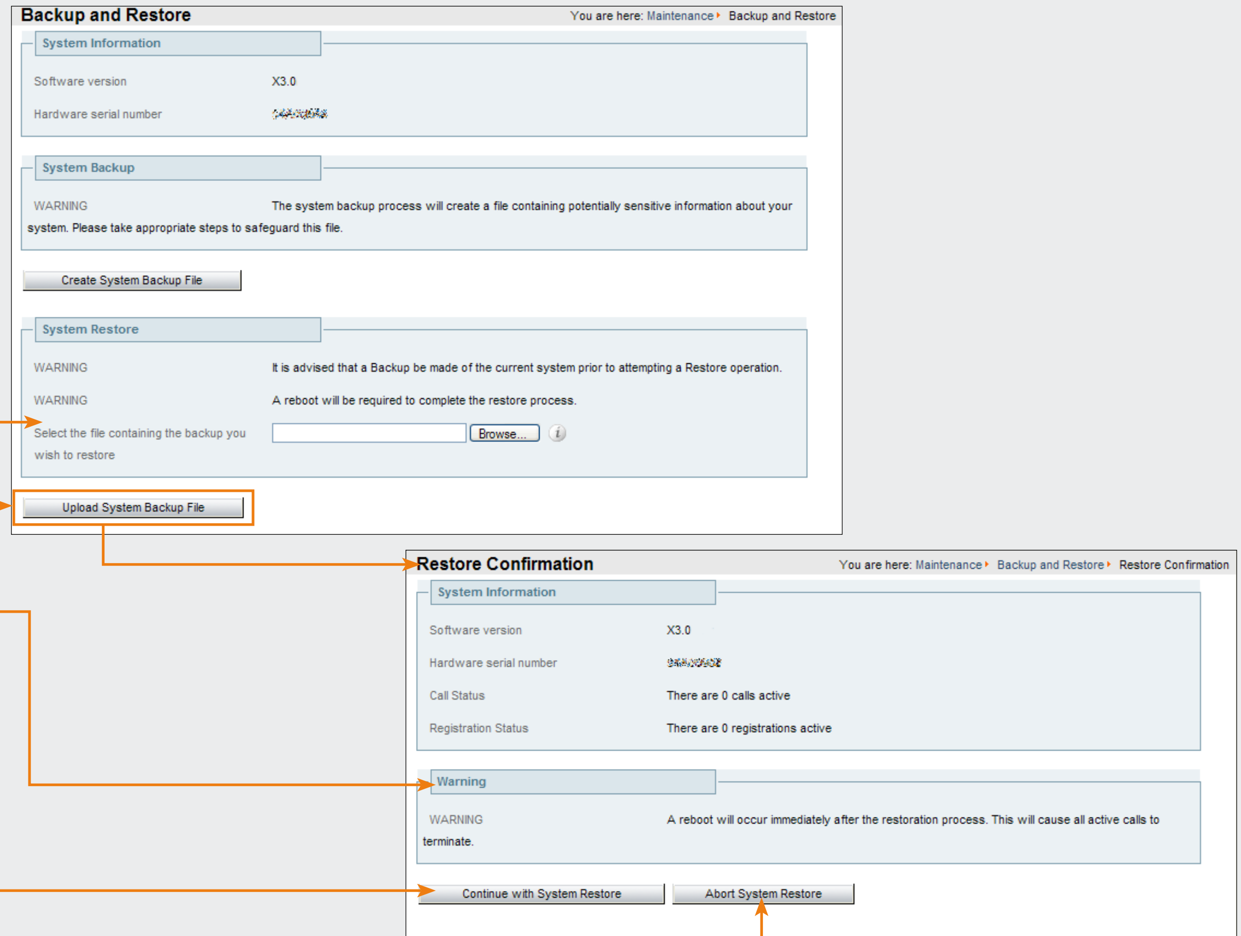
Continue with System Restore

Click here to continue with the restore process. This will restart your system, so ensure that there are no active calls.

Once the system has restarted, you will be taken to the login page.

Abort System Restore

Click here to exit the restore process and return to the Backup and Restore page.



System Snapshot

Overview

The system snapshot is used for diagnostic purposes. It is a file that can be sent to your TANDBERG support representative at their request to assist them in troubleshooting issues you may be experiencing.

To create a system snapshot file:

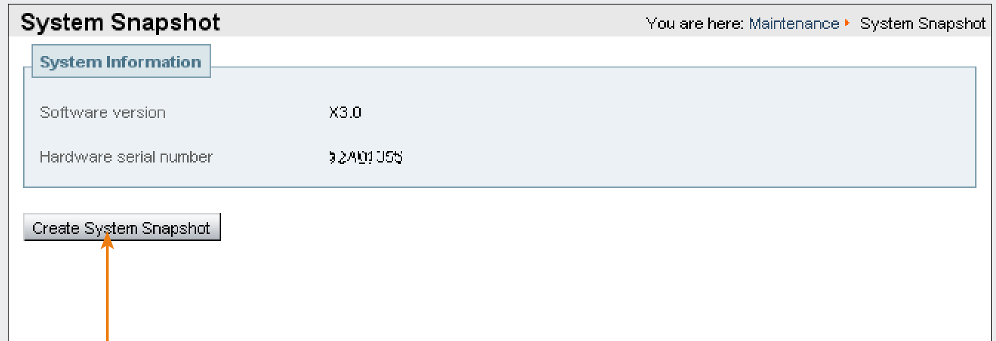
- Maintenance > System Snapshot.
  You will be taken to the System Snapshot page.

Create System Snapshot

Clicking on this button will initiate the download of the system snapshot file. You will then be asked whether and where you would like to save the file.

Select a location from which you can easily send the file to your TANDBERG support representative.

Creating a System Snapshot



Error Reports

You can configure the VCS to automatically send reports to a specified web service each time it experiences application failures such as system crashes. The information contained in these reports can then be used by TANDBERG technical support to diagnose the cause of the failures. This feature is only intended for use at the request of TANDBERG technical support in exceptional situations, and is OFF by default. This feature cannot be configured via the web interface; it is configured via `xConfiguration Error Reports`.

Restarting

Overview

Some configuration changes will require a restart of the VCS before they take effect. There will be a Restart button at the bottom of any web pages that include such options, and clicking on this button will take you to the Restart page. If you do not restart the system after making these changes, you will receive a warning telling you the system needs to be restarted.

Restarting will cause any active calls and registrations to be terminated. For this reason, the Restart page displays the number of current calls and registrations, so you can check these before you restart.

If you do not restart the system immediately, you should refresh this page before restarting to check the current status of calls and registrations.

Do not restart the system while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your TANDBERG representative.

To restart the VCS:

- Maintenance > Restart.
  You will be taken to the Restart page.
- From any configuration page, click the Restart button.
  You will be taken to the Restart page.
- `xCommand Boot`

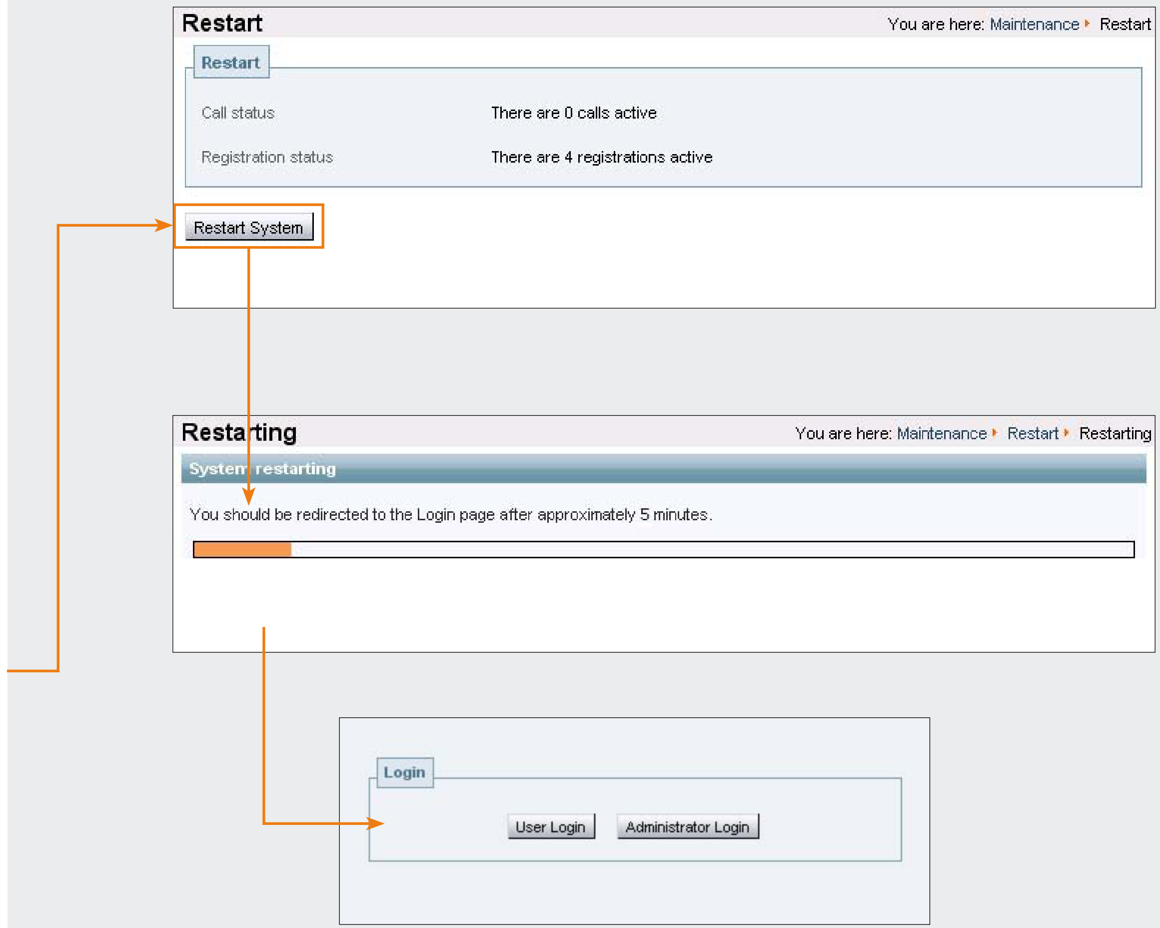
Restart System

Click here to restart the system.

The Restarting page will appear, with an orange bar indicating progress.

Once the system has successfully restarted, you will automatically be taken to the Login page.

Restarting the VCS



Shutting Down

Overview

The system must be shut down before it is unplugged.

Once the system has been shut down, the only way it can be restarted is by pressing the soft power button on the unit itself. You must therefore have physical access to the unit if you wish to be able to restart it after it has been shut down.

Shutting down will cause any active calls and registrations to be terminated. For this reason, the Shutdown page displays the number of current calls and registrations, so you can check these before you shut down.

If you do not shut down the system immediately, you should refresh this page before shutting down to check the current status of calls and registrations.

Do not shut down the system while the red ALM LED on the front of the box is on. This indicates a hardware fault. Contact your TANDBERG representative.

To shut down the VCS:

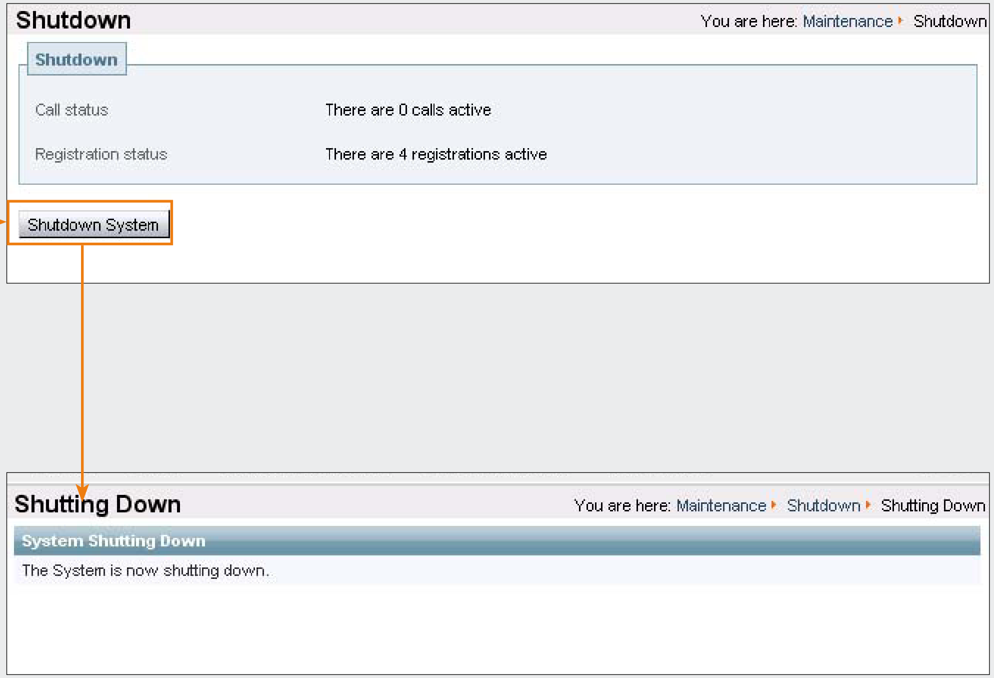
- Maintenance > Shutdown.
  You will be taken to the Shutdown page.

Shutdown System

Click here to shut down the system.

The Shutting Down page will appear. This page will remain in place once the system has successfully shut down but any attempts to refresh the page or access the VCS will then be unsuccessful.

Shutting Down



Restoring Default Configuration

Overview

It is possible to restore the VCS to its default configuration. This is done via the CLI using xCommand DefaultValuesSet. This command is not available via the web UI.

The DefaultValuesSet command allows you to specify the level of configuration to restore, from 1 to 3 as follows:

- Level 1 resets most configuration items to their default value, with the exception of the items shown in the table opposite. The xConfiguration reference table shows a full list of all configuration items and where applicable their default values.
- Level 2 is not currently used, so setting this level has the same effect as setting Level 1.
- Level 3 resets all configuration items to their default value, including those shown in the table opposite.

xCommand DefaultValuesSet Level: 3 must be used with caution, as it resets the system's IPv4 and IPv6 addresses, meaning you will no longer be able to access the system over IP. It also deletes all option keys including pre-installed options such as Expressway and the number of registrations and calls.

DefaultValuesSet Level 3

Configuration item	Default value after xCommand DefaultValuesSet Level: 3
SystemUnit Name	<blank>
SystemUnit Password	TANDBERG
Option [1..64] Key	<all option keys are deleted>
IPProtocol	IPv4
IP Gateway	127.0.0.1
IP V6 Gateway	<blank>
IP DNS Server [1..5] Address	<blank>
IP DNS Domain Name	<blank>
Ethernet [1..2] Speed	Auto
Ethernet [1..2] IP V4 Address	192.168.0.100
Ethernet [1..2] IP V4 SubnetMask	255.255.255.0
Ethernet [1..2] IP V6 Address	<blank>
NTP Address	<blank>
SNMP Mode	Off
SNMP CommunityName	public
SNMP SystemContact	<blank>
SNMP SystemLocation	<blank>
Administration TimeOut	0
ExternalManager Address	<blank>
ExternalManager Path	tms/public/external/management/SystemManagementService.asmx
Policy AdministratorPolicy Mode	Off
Policy UserPolicy Mode	Local
Policy UserPolicy Server Protocol	HTTP
Policy UserPolicy Server Address	<blank>
Policy UserPolicy Server Path	<blank>
Policy UserPolicy Server UserName	<blank>
Policy UserPolicy Server Password	<blank>

Password Encryption

Overview

All passwords configured on the VCS are stored in encrypted form. This applies to the following, which all have usernames and passwords associated with them:

- the default admin administrator account
- any additional administration accounts
- local database authentication credentials (a list of valid usernames and passwords that are used when other devices are required to authenticate with the VCS)
- external registration authentication credentials (used by the VCS when required to authenticate with another system)
- LDAP server (used by the VCS when binding to an LDAP server)

Passwords can be configured via either the CLI or the web interface.

Web Interface

When entering or viewing passwords via the web interface, you will see placeholder characters (e.g. dots or stars, depending on your browser) instead of the characters you are typing.

Command Line Interface

When entering passwords via the Command Line Interface (CLI), you will type the password in plain text. However, once the command has been executed, the password will be displayed in its encrypted form with a `{cipher}` prefix, e.g.

```
xConfiguration LDAP Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="
```

FindMe is a stand-alone application that can be hosted by the VCS or by another remote server. This means that FindMe user account information is not configured or accessible via the CLI of the VCS. However, FindMe user passwords are still stored securely.

Maximum length of Passwords

When a password is encrypted, it uses more characters than the original plain text version of the password. The maximum number of encrypted and plain text characters for each type of password is shown in the table below.

Password type	Maximum plain text characters	Maximum encrypted characters
Admin account	16	65
Administration accounts	16	65
Local Database authentication credentials	128	215
External authentication credentials	128	215
LDAP server	60	122
FindMe Remote User Policy Manager	30	82

Appendices

This section includes the following appendices which provide supplementary information regarding the administration of the VCS:



Overview of CPL on the VCS

This Appendix gives details of the VCS's implementation of the CPL language and should be read in conjunction with the CPL standard RFC 3880 [5] and the TANDBERG guide to writing CPL [22].

The VCS supports most of the CPL standard along with some TANDBERG-defined extensions. It does not support the top level actions <incoming> and <outgoing> as described in RFC 3880. Instead it supports a single section of CPL within a <routed> section.

When Administrator Policy is implemented by uploading a CPL script to the VCS, the script is checked against an XML schema to verify the syntax. There are two schemas - one for the basic CPL specification and one for the TANDBERG extensions. Both these schemas can be downloaded from the web interface and used to validate your script before uploading to the VCS.

The following example shows the correct use of namespaces to make the syntax acceptable:

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
<taa:routed>
  <address-switch field="destination">
    <address is="reception@example.com">
      <proxy/>
    </address>
  </address-switch>
</taa:routed>
</cpl>
```

address-switch

Overview

The address-switch node allows the script to run different actions based on the source or destination aliases of the call. It specifies which fields to match, and then a list of address nodes contains the possible matches and their associated actions.

The address-switch has two node parameters: Field and Subfield.

address

The address construct is used within an address-switch to specify addresses to match. It supports the use of Regular Expressions (see the Regular Expression Reference for further information).

Valid values are:

`is=string`	Selected field and subfield exactly match the given string.
`contains=string`	Selected field and subfield contain the given string. Note: The CPL standard only allows for this matching on the display subfield; however the VCS allows it on any type of field.
`subdomain-of=string`	If the selected field is numeric (e.g. the tel subfield) then this matches as a prefix; so `address subdomain-of="555"` matches `5556734` etc. If the field is not numeric then normal domain name matching is applied; so `address subdomain-of="company.com"` matches `nodeA.company.com` etc.
`regex="regular expression"`	Selected field and subfield match the given regular expression.

All address comparisons ignore upper/lower case differences so `address is="Fred"` will also match `fred`, `freD` etc.

address-switch

field

Within the address-switch node, the mandatory field parameter specifies which address is to be considered. The supported attributes and their interpretation are as follows:

	Authentication Mode: On		Authentication Mode: Off	
Field	SIP	H.323	SIP	H.323
origin	The "From" and "ReplyTo" fields of the message if it authenticated correctly, otherwise not-present.	The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly otherwise not-present. Since SETUP messages are not authenticated if we receive a setup without a preceding RAS message the origin will always be not-present.	The "From" and "ReplyTo" fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.
unauthenticated-origin	The "From" and "ReplyTo" fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.	The "From" and "ReplyTo" fields of the incoming message.	The source aliases from the original LRQ or ARQ that started the call. If a SETUP is received without a preceding RAS message then the origin is taken from the SETUP.
authenticated-origin	The "From" and "ReplyTo" fields of the message if it authenticated correctly, otherwise not-present.	The source aliases from the original LRQ or ARQ that started the call if it authenticated correctly otherwise empty. Since SETUP messages are not authenticated if we receive a setup without a preceding RAS message the origin will always be not-present.	not-present	
originating-zone	The name of the zone or subzone for the originating leg of the call. If the call originates from a Neighbor, Traversal Server or Traversal Client zone then this will equate to the zone name. If it comes from an endpoint within one of the local subzones this will be the name of the subzone. If the call originates from any other locally registered endpoint this will be "DefaultSubZone". In all other cases this will be "DefaultZone".			
originating-user	The username used for authentication.		not-present	
registered-origin	If the call originates from a registered endpoint this is the list of all aliases it has registered, otherwise not-present.			
destination	The destination aliases.			
original-destination	The destination aliases.			

If the selected field contains multiple aliases then the VCS will attempt to match each address node with all of the aliases before proceeding to the next address node i.e. an address node matches if it matches any alias.

address-switch

subfield

Within the address-switch node, the optional subfield parameter specifies which part of the address is to be considered. The following table gives the definition of subfields for each alias type.

If a subfield is not specified for the alias type being matched then the `not-present` action will be taken.

`address-type`	Either `h323` or `sip`, based on the type of endpoint that originated the call.
`user`	For URI aliases this selects the username part. For H.323 IDs it is the entire ID and for E.164 numbers it is the entire number.
`host`	For URI aliases this selects the domain name part. If the alias is an IP address then this subfield is the complete address in dotted decimal form.
`tel`	For E.164 numbers this selects the entire string of digits.
`alias-type`	Gives a string representation of the type of alias. The type is inferred from the format of the alias. Possible types are: • Address Type • Result • URI • url-ID • H.323 ID • h323-ID • Dialed Digits • dialedDigits

otherwise

The otherwise node will be executed if the address specified in the address-switch was found but none of the preceding address nodes matched.

not-present

The not-present node is executed when the address specified in the address-switch was not present in the call setup message. This form is most useful when authentication is being used. With authentication enabled the VCS will only use authenticated aliases when running policy so the not-present action can be used to take appropriate action when a call is received from an unauthenticated user (see the example Call Screening of Unauthenticated Users).

location

As the CPL script is evaluated it maintains a list of addresses (H.323 IDs, URLs and E.164 numbers) which will be used as the destination of the call if a proxy node is executed. The location node allows the location set to be modified so that calls can be redirected to different destinations.

At the start of script execution the location set is initialized to empty for incoming calls and to the original destination for outgoing calls.

The following attributes are supported on location nodes. It supports the use of Regular Expressions (see the Regular Expression Reference for further information).

Clear = "yes" | "no"	Specifies whether to clear the current location set before adding the new location. The default is to append this location to the end of the set.
url=string	The new location to be added to the location set. The given string can specify a URL (e.g. user@domain.com), H.323 ID or an E.164 number.
priority=<0.0..1.0> | "random"	Specified either as a floating point number in the range 0.0 to 1.0, or random, which assigns a random number within the same range. 1.0 is the highest priority. Locations with the same priority are searched in parallel.
regex="<regular expression>" replace="<string>"	Specifies the way in which a location matching the regular expression is to be changed.

rule-switch

This extension to CPL is provided to simplify administrator policy scripts that need to make decisions based on both the source and destination of the call. A rule-switch may contain any number of rules that are tested in sequence; as soon as a match is found the CPL within that rule element is executed. Each rule must take one of the following forms:

```
<rule origin="<regular expression>" destination="<regular expression">
<rule authenticated-origin="<regular expression>" destination="<regular expression">
<rule unauthenticated-origin="<regular expression>" destination="<regular expression">
<rule registered-origin="<regular expression>" destination="<regular expression">
<rule originating-user="<regular expression>" destination="<regular expression">
<rule originating-zone="<regular expression>" destination="<regular expression">
```

The meaning of the various origin selectors is as described in the Field section.

proxy

On executing a proxy node the VCS will attempt to forward the call to the locations specified in the current location set. If multiple entries are in the location set then this results in a forked call. If the current location set is empty the call will be forwarded to its original destination.

reject

If a reject node is executed the VCS stops any further script processing and rejects the current call. The custom reject strings status=string and reason=string options are supported here.

Unsupported CPL Elements

The VCS does not currently support some elements that are described in the CPL RFC. If an attempt is made to upload a script containing any of the following elements an error message will be generated and the VCS will continue to use its existing policy.

The following elements are not currently supported:

- time-switch
- string-switch
- language-switch
- priority-switch
- redirect
- mail
- log
- subaction
- lookup
- remove-location

CPL Examples

Call Screening of Authenticated Users

In this example, only calls from users with authenticated source addresses are allowed. See the section on Authentication for details on how to enable authentication.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="origin">
      <not-present>
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="Denied by policy"/>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

Call Screening Based on Alias

In this example, user ceo will only accept calls from users vpsales, vpmarketing or vpengineering.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="destination">
      <address is="ceo">
        <address-switch field="origin">
          <address regex="vpsales|vpmarketing|vpengineering">
            <!-- Allow the call -->
            <proxy/>
          </address>
          <not-present>
            <!-- Unauthenticated user -->
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </not-present>
          <otherwise>
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </otherwise>
        </address-switch>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Examples

Call Screening Based on Domain

In this example, user fred will not accept calls from anyone at annoying.com, or from any unauthenticated users. All other users will allow any calls.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="destination">
      <address is="fred">
        <address-switch field="origin" subfield="host">
          <address subdomain-of="annoying.com">
            <!-- Don't accept calls from this source -->
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <not-present>
            <!-- Don't accept calls from unauthenticated sources -->
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </not-present>
          <otherwise>
            <!-- All other calls allowed -->
            <proxy/>
          </otherwise>
        </address-switch>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

Change of Domain Name

In this example, Example Inc has changed its domain from example.net to example.com. For a period of time some users are still registered at example.net. The following script would attempt to connect calls to user@example.com first and if that fails then fallback to example.net.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="destination">
      <address regex="(.*)@example.com">
        <proxy>
          <failure>
            <!-- Failed to contact using example.com, retry the request
with example.net -->
            <taa:location clear="yes" regex="(.*)@example.com"
replace="\1@example.net">
              <proxy/>
            </taa:location>
          </failure>
        </proxy>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Examples

Allow Calls from Locally Registered Endpoints Only

In this example, the administrator only wants to allow calls that originate from locally registered endpoints.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="registered-origin">
      <not-present>
        <reject status="403" reason="Only local endpoints can use this
Tandberg VCS"/>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

Block Calls from Default Zone and Default Subzone

The same script can be extended to also allow calls from configured zones but not from the Default Zone or Default Subzone.

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="registered-origin">
      <not-present>
        <address-switch field="originating-zone">
          <address is="DefaultZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <address is="DefaultSubZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
          <otherwise>
            <proxy/>
          </otherwise>
        </address-switch>
      </not-present>
    </address-switch>
  </taa:routed>
</cpl>
```

CPL Examples

Restricting Access to a Local Gateway

In these examples, a gateway is registered to the VCS with a prefix of `9` and the administrator wants to stop calls from outside the organization being routed through it.

We can do this in two ways: using the `address-switch` node or the `rule-switch` node. Examples of each are shown below.

Using the address-switch node

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <address-switch field="destination">
      <address regex="9(.*)">
        <address-switch field="originating-zone">
          <!-- Calls coming from the traversal zone are not allowed to use
this gateway -->
          <address is="TraversalZone">
            <!-- Reject call with a status code of 403 (Forbidden) -->
            <reject status="403" reason="Denied by policy"/>
          </address>
        </address-switch>
      </address>
    </address-switch>
  </taa:routed>
</cpl>
```

Using the rule-switch node

```
<?xml version="1.0" encoding="UTF-8" ?>
<cpl xmlns="urn:ietf:params:xml:ns:cpl"
     xmlns:taa="http://www.tandberg.net/cpl-extensions"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="urn:ietf:params:xml:ns:cpl cpl.xsd">
  <taa:routed>
    <taa:rule-switch>
      <taa:rule originating-zone="TraversalZone" destination="9(.*)">
        <!-- Calls coming from the traversal zone are not allowed to use
this gateway -->
        <!-- Reject call with a status code of 403 (Forbidden) -->
        <reject status="403" reason="Denied by policy"/>
      </taa:rule>
      <taa:rule origin="(.*)" destination="(.*)">
        <!-- All other calls allowed -->
        <proxy/>
      </taa:rule>
    </taa:rule-switch>
  </taa:routed>
</cpl>
```

Regular Expression Reference

Overview

Regular expressions can be used in conjunction with a number of VCS features such as alias transformations, zone transformations, CPL policy and ENUM. The VCS uses POSIX format regular expression syntax.

The table opposite provides a list of commonly used special characters in regular expression syntax. This is only a subset of the full range of expressions available. For a detailed description of regular expression syntax see the publication Mastering Regular Expressions [9].

For an example of regular expression usage, see the section CPL Examples.

Common Regular Expressions

Character	Description	Example
.	Matches any single character.	
*	Matches 0 or more repetitions of the previous match.	.* will match against any sequence of characters.
+	Matches 1 or more repetitions of the previous match.	
\	Escapes a regular expression special character.	
\d	Matches any decimal digit, i.e. 0-9.	
[...]	Matches a set of characters. Each character in the set can be specified individually, or a range can be specified by giving the first character in the range followed by the - character and then the last character in the range. You can not use special characters within the [] - they will be taken literally.	[a-z] will match against any lower case alphabetical character. [a-zA-Z] will match against any alphabetical character. [0-9#*] will match against any single E.164 character - the E.164 character set is made up of the digits 0-9 plus the hash key (#) and the asterisk key (*).
(...)	Groups a set of matching characters together. Groups can then be referenced in order using the characters \1, \2, etc. as part of a replace string.	A regular expression can be constructed to transform a URI containing a user's full name to a URI based on their initials. The regular expression (.).*_(.).*(@example.com) would match against the user john_smith@example.com and with a replace string of \1\2\3 would transform it to js@example.com.
|	Matches against one expression or an alternate expression.	.*@example.(net|com) will match against any URI for the domain example.com or the domain example.net.
^	Signifies the start of a line. When used immediately after an opening brace, negates the character set inside the brace.	[^abc] matches any single character that is NOT one of a, b or c.
$	Signifies the end of a line.	^\d\d\d$ will match any string that is exactly 3 digits long.
(?!...)	Negative lookahead. Defines a subexpression that *must not* be present in order for there to be a match.	(?!.*@tandberg.net$).* will match any string that does not end with @tandberg.net.

Pattern Variable Reference

Overview

The VCS makes use of pattern matching in a number of its features, namely Allow Lists and Deny Lists, pre-search Transforms and Zone Transforms.

For each of these pattern matches, the VCS allows you to use a variable that it will replace with the current configuration value(s) before the pattern is checked.

These variables can be used as either or both of:

- all or part of the pattern that is being searched for
- all or part of the string that is replacing the pattern that was found.

The variables can be used in all types of patterns, i.e. prefix, suffix, regex and exact.

The table opposite shows the strings that are valid as variables, and the values they represent.

Valid Variable Strings

String	Equals current value(s) returned by...	When used in a Match field	When used in a Replace field
%ip%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V4 Address xConfiguration Ethernet 2 IP V6 Address	Matches all IPv4 and IPv6 addresses currently configured on the VCS.	not applicable
%ipv4%	xConfiguration Ethernet 1 IP V4 Address xConfiguration Ethernet 2 IP V4 Address	Matches the IPv4 addresses currently configured on the VCS for LAN 1 and LAN 2.	not applicable
%ipv4_1%	xConfiguration Ethernet 1 IP V4 Address	Matches all IPv4 address currently configured on the VCS for LAN 1.	Replaces the string with the LAN 1 IPv4 address.
%ipv4_2%	xConfiguration Ethernet 2 IP V4 Address	Matches all IPv4 address currently configured on the VCS for LAN 2.	Replaces the string with the LAN 2 IPv4 address.
%ipv6%	xConfiguration Ethernet 1 IP V6 Address xConfiguration Ethernet 2 IP V6 Address	Matches the IPv6 addresses currently configured on the VCS for LAN 1 and LAN 2.	not applicable
%ipv6_1%	xConfiguration Ethernet 1 IP V6 Address	Matches the IPv6 address currently configured on the VCS for LAN 1.	Replaces the string with the LAN 1 IPv6 address.
%ipv6_2%	xConfiguration Ethernet 2 IP V6 Address	Matches the IPv6 address currently configured on the VCS for LAN 2.	Replaces the string with the LAN 2 IPv6 address.
%localdomains%	xConfiguration SIP Domains Domain 1 Name ... xConfiguration SIP Domains Domain 20 Name	Matches all the SIP domains currently configured on the VCS.	not applicable
%localdomain1% ... %localdomain20%	xConfiguration SIP Domains Domain 1 Name ... xConfiguration SIP Domains Domain 20 Name	Matches the specified SIP domain. Up to 20 SIP domains can be configured on the VCS, and they are identified by an index number between 1 and 20.	Replaces the string with the specified SIP domain.
%systemname%	xConfiguration SystemUnit Name	Matches the VCS's System Name.	Replaces the string with the VCS's System Name.

VCS Port Reference

Overview

The VCS uses different ports and protocols for different services and functions, and many of these are configurable.

The table below shows all the ports on the VCS that are used for each of these services and functions. It shows the default port(s) and protocol used, and if the ports are configurable it shows the available range and how to configure them via the web UI or CLI.

Two services or functions cannot share the same port and protocol; if you attempt to change an existing port or range and it conflicts with another service, you will get a warning message.

VCS Ports

Service/Function	Description	Default	Available Range	Configurable via
SSH and FindMe replication for Clusters	for encrypted command line administration. Also used to replicate FindMe data if the VCS is part of a cluster with FindMe enabled.	22 TCP	not configurable	
Telnet	used for unencrypted command line administration	23 TCP	not configurable	
HTTP	used for unencrypted Web administration	80 TCP	not configurable	
SNMP	used for network management	161 UDP	not configurable	
NTP	used for updating the system time (and important for H.235 security)	123 UDP	not configurable	
Reserved for future use		389		
HTTPS	used for encrypted Web administration. Also used to replicate FindMe data if the VCS is part of a cluster with FindMe enabled.	443 TCP	not configurable	
Remote Logging	used to send message to the remote syslog server	514 UDP	not configurable	
Reserved for future use		636		
Gatekeeper discovery	Multicast Gatekeeper discovery	1718 UDP	not configurable	
H323 Registration and Clustering	used to listen for inbound H.323 UDP registrations. If the VCS is part of a cluster, this port is also used for inbound and outbound communication with Peers, even if H.323 is disabled	1719 UDP	1024 - 65534	VCS Configuration > Protocols > H.323 `xConfiguration H323 Gatekeeper Registration UDP Port`
H.323 call signaling	listens for H.323 call signaling	1720 TCP	1024 - 65534	VCS Configuration > Protocols > H.323 `xConfiguration H323 Gatekeeper CallSignaling TCP Port`

VCS Ports

Service/Function	Description	Default	Available Range	Configurable via
Traversal Server Media Demultiplexing RTP	used on the VCS Expressway for demultiplexing RTP media	2776 UDP	1024 - 65534	VCS Configuration > Expressway > Ports xConfiguration Traversal Server Media Demultiplexing RTP Port
Assent call signaling	used on the VCS Expressway for Assent signaling	2776 TCP	1024 - 65534	VCS Configuration > Expressway > Ports xConfiguration Traversal Server H323 Assent CallSignaling Port
H.460.18 call signaling	used on the VCS Expressway for H.460.18 signaling	2777 TCP	1024 - 65534	VCS Configuration > Expressway > Ports xConfiguration Traversal Server H323 H46018 CallSignaling Port
Traversal Server Media Demultiplexing RTCP	used on the VCS Expressway for demultiplexing RTCP media	2777 UDP	1024 - 65534	VCS Configuration > Expressway > Ports xConfiguration Traversal Server Media Demultiplexing RTCP Port
STUN Discovery	used on the VCS Expressway for STUN discovery services	3478 UDP	1024 - 65534	VCS Configuration > Expressway > STUN xConfiguration Traversal Server STUN Discovery Port
STUN Relay	used on the VCS Expressway listening port for STUN relay requests.	4678 UDP	1024 - 65534	VCS Configuration > Expressway > STUN xConfiguration Traversal Server STUN Relay Port
SIP UDP	listens for incoming SIP UDP calls	5060 UDP	1024 - 65534	VCS Configuration > Protocols > SIP > Configuration xConfiguration SIP UDP Port
SIP TCP	listens for incoming SIP TCP calls.	5060 TCP	1024 - 65534	VCS Configuration > Protocols > SIP > Configuration xConfiguration SIP TCP Port
SIP TLS	listens for incoming SIP TLS calls	5061 TLS	1024 - 65534	VCS Configuration > Protocols > SIP > Configuration xConfiguration SIP TLS Port
Traversal Server Zone H323 Port	the port on the VCS Expressway being used for H.323 firewall traversal from a particular traversal client.	6001 UDP, incrementing by 1 for each new zone.	1024 - 65534	VCS Configuration > Zones > Edit Zone xConfiguration Zones Zone [1..200] TraversalServer H323 Port
Traversal Server Zone SIP Port	the port on the VCS Expressway being used for SIP firewall traversal from a particular traversal client.	7001 TCP/TLS, incrementing by 1 for each new zone.	1024 - 65534	VCS Configuration > Zones > Edit Zone xConfiguration Zones Zone [1..200] TraversalServer SIP Port
Reserved for future use		8989		
DNS	used for sending requests to DNS servers	10000 - 10210 UDP	not configurable	
H.225 and H.245 call signaling port range	the range of ports to be used for call signalling once a call is established	15000 - 19999 TCP	1024 - 65534	VCS Configuration > Protocols > H.323 xConfiguration H323 Gatekeeper CallSignaling PortRange Start xConfiguration H323 Gatekeeper CallSignaling PortRange End

VCS Ports

Service/Function	Description	Default	Available Range	Configurable via
SIP TCP outbound port range	The range of ports to be used by outbound TCP/TLS SIP connections to a remote SIP device	25000 - 29999 TCP/TLS	1024 - 65533	VCS Configuration > Protocols > SIP > Configuration xConfiguration SIP TCP Outbound Port Start xConfiguration SIP TCP Outbound Port End
Traversal media port range	For traversal calls (i.e. where the VCS is taking the media as well as the signaling), the range of ports to be used for the media. Ports are allocated from this range in pairs, the first of each being even. Therefore the range must start with an even number. See Configuring the Traversal Subzone Ports for more information.	50000 - 51199 UDP	1024 - 65533	VCS Configuration > Local Zone > Traversal Subzone xConfiguration Traversal Media Port Start xConfiguration Traversal Media Port End
STUN Relay media port range	The range of ports to be used for STUN media relay.	60000 - 61200 UDP	1024 - 65534	VCS Configuration > Expressway > STUN xConfiguration Traversal Server STUN Relay Media Port Start xConfiguration Traversal Server STUN Relay Media Port End
LDAP	used for outbound connection to an LDAP server (if the VCS is configured to use an LDAP server for H.350 authentication)	a random TCP source port is used		
TMS	used for outbound connection to TMS	a random source port in the range 32768 - 65535 is used		
User Policy Server	used for outbound connection to a User Policy Server	a random source port in the range 32768 - 65535 is used		

DNS Configuration

Overview

This section gives examples of DNS configuration using Microsoft DNS Server and BIND 8 & 9.

In these examples we show how to set up an SRV record to handle H.323 URIs of the form user@example.com. These are handled by the system with the fully qualified domain name of vcs.example.com which is listening on port 1719, the default registration port.

It is assumed that both A and AAAA records already exist for vcs.example.com. If not, you will need to add one.

Verifying the SRV Record

There are a range of tools available to investigate DNS records. One commonly found on Microsoft Windows and UNIX platforms is `nslookup`. Use this to verify that everything is working as expected.

For example:

- `nslookup -querytype=srv _h323ls._udp.example.com`

and check the output.

Microsoft DNS Server

Using Microsoft DNS Server you can add the SRV record using either the command line or the MMC snap-in.

To use the command line, on the DNS server open a command window and enter:

- `dnscmd . /RecordAdd domain service_name SRV Priority Weight Port Target`

where:

`domain`	is the domain into which you wish to insert the record
`service_name`	is the name of the service you're adding
`Priority`	is the priority as defined by RFC 2782 [3]
`Weight`	is the weight as defined by RFC 2782 [3]
`Port`	is the port on which the system hosting the domain is listening
`Target`	is the FQDN of the system hosting the domain

For example:

- `dnscmd . /RecordAdd example.com _h323ls._udp SRV 1 0 1719 vcs.example.com`

BIND 8 & 9

BIND is a commonly used DNS server on UNIX and Linux systems. Configuration is based around two sets of text files: `named.conf` which describes which zones are represented by the server, and a selection of zone files which describe the detail of each zone.

BIND is sometimes run chrooted for increased security. This gives the program a new root directory, which means that the configuration files may not appear where you expect them to be. To see if this is the case on your system, run

- `ps aux | grep named`

This will give the command line that named (the BIND server) was invoked with. If there is a `-t` option, then the path following that is the new root directory and your files will be located relative to that root.

In `/etc/named.conf` look for a directory entry within the options section. This will give the directory in which the zone files are stored, possibly relative to a new root directory. In the appropriate zone section, a file entry will give the name of the file containing the zone details.

For more details of how to configure BIND servers and the DNS system in general see the publication DNS and BIND [6].

LDAP Configuration

About the LDAP Databases

The VCS can be configured to use a database on an LDAP Directory Server to store authentication credential information (usernames, passwords, and other relevant information)

This section describes how to download the schemas that must be installed on the LDAP server, and how to install and configure two common types of LDAP servers, Microsoft Active Directory and OpenLDAP, for use with the VCS.

Downloading the LDAP schemas

The following ITU specification describes the schemas which are required to be installed on the LDAP server:

H.350	Directory services architecture for multimedia conferencing - An LDAP schema to represent endpoints on the network.
H.350.1	Directory services architecture for H.323 - An LDAP schema to represent H.323 endpoints.
H.350.2	Directory services architecture for H.235 - An LDAP schema to represent H.235 elements.

The schemas can be downloaded in `ldif` format from the web interface on the VCS. To do this:

1. Navigate to VCS Configuration > Authentication > LDAP > Schemas. You will see a list of downloadable schemas.
2. Click on the Download button next to each file to open it.

Microsoft Active Directory

Prerequisites

These step-by-step instructions assume that Active Directory has already been installed. For details on installing Active Directory please consult your Windows documentation.

The following instructions are for Windows Server 2003 Enterprise Edition. If you are not using this version of Windows, your instructions may vary.

Installing the H.350 Schemas

Once you have downloaded the H.350 schemas, install them as follows:

Open a command prompt and for each file execute the following command:

```
ldifde -i -c DC=X <ldap_base> -f filename.ldf
```

where:

`<ldap_base>` is the base DN for your Active Directory server.

Microsoft Active Directory

Adding H.350 Objects

Create the Organizational Hierarchy

1. Open up the Active Directory Users and Computers MMC snap-in.
2. Under your BaseDN right-click and select New Organizational Unit.
3. Create an Organizational unit called h350.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the VCS read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 Objects

1. Create an `ldif` file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,DC=X
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@X
```

2. Add the ldif file to the server using the command:

```
ldifde -i -c DC=X <ldap _ base> -f filename.ldf
```

where:

`<ldap _ base>` is the base DN of your Active Directory Server.

The example above will add a single endpoint with an H.323 ID alias of MeetingRoom1, an E.164 alias of 626262 and a SIP URI of MeetingRoom@X The entry also has H.235 and SIP credentials of ID meetingroom1 and password mypassword which are used during authentication.

H.323 registrations will look for the H.323 and H.235 attributes; SIP will look for the SIP attributes. Therefore if your endpoint is registering with just one protocol you do not need to include elements relating to the other.

The SIP URI in the `ldif` file must be prefixed by `sip:`.

For information about what happens when an alias is not in the LDAP database see the section Alias Origin Setting.

Securing with TLS

To enable Active Directory to use TLS, you must request and install a certificate on the Active Directory server. The certificate must meet the following requirements:

- Be located in the Local Computer's Personal certificate store. This can be seen using the Certificates MMC snap-in.
- Have the private details on how to obtain a key associated for use with it stored locally. When viewing the certificate you should see a message saying "You have a private key that corresponds to this certificate''.
- Have a private key that does not have strong private key protection enabled. This is an attribute that can be added to a key request.
- The Enhanced Key Usage extension includes the Server Authentication object identifier, again this forms part of the key request.
- Issued by a CA that both the domain controller and the client trust.
- Include the Active Directory fully qualified domain name of the domain controller in the common name in the subject field and/or the DNS entry in the subject alternative name extension.

To configure the VCS to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the VCS by navigating to:

- Maintenance > Security.

OpenLDAP

Prerequisites

These instructions assume that an OpenLDAP server has already been installed. For details on installing OpenLDAP see the documentation at http://www.openldap.org.

The following examples use a standard OpenLDAP installation on the Linux platform. For installations on other platforms the location of the OpenLDAP configuration files may be different. See the OpenLDAP installation documentation for details.

Installing the H.350 Schemas

1. Copy the OpenLDAP files to the OpenLDAP schema directory:

```
/etc/openldap/schemas/commobject.ldif
/etc/openldap/schemas/h323identity.ldif
/etc/openldap/schemas/h235identity.ldif
/etc/openldap/schemas/sipidentity.ldif
```

2. Edit `/etc/openldap/slapd.conf` to add the new schemas. You will need to add the following lines:

```
include /etc/openldap/schemas/commobject.ldif
include /etc/openldap/schemas/h323identity.ldif
include /etc/openldap/schemas/h235identity.ldif
include /etc/openldap/schemas/sipidentity.ldif
```

The OpenLDAP daemon (`slapd`) must be restarted for the new schemas to take effect.

OpenLDAP

Adding H.350 Objects

Create the Organizational Hierarchy

1. Create an ldif file with the following contents:

```
# This example creates a single
# organizational unit to contain the H.350
# objects
dn: ou=h350,dc=my-domain,dc=com
objectClass: organizationalUnit
ou: h350
```

2. Add the ldif file to the server using the command:

```
slapadd -l <ldif_file>
```

This organizational unit will form the BaseDN to which the VCS will issue searches. In this example the BaseDN will be: ou=h350,dc=my-domain,dc=com.

It is good practice to keep the H.350 directory in its own organizational unit to separate out H.350 objects from other types of objects. This allows access controls to be setup which only allow the VCS read access to the BaseDN and therefore limit access to other sections of the directory.

Add the H.350 Objects

1. Create an ldif file with the following contents:

```
# MeetingRoom1 endpoint
dn: commUniqueId=comm1,ou=h350,dc=my-domain,dc=com
objectClass: commObject
objectClass: h323Identity
objectClass: h235Identity
objectClass: SIPIdentity
commUniqueId: comm1
h323Identityh323-ID: MeetingRoom1
h323IdentitydialedDigits: 626262
h235IdentityEndpointID: meetingroom1
h235IdentityPassword: mypassword
SIPIdentityUserName: meetingroom1
SIPIdentityPassword: mypassword
SIPIdentitySIPURI: sip:MeetingRoom@domain.com
```

2. Add the ldif file to the server using the command:

```
slapadd -l <ldif_file>
```

The example above will add a single endpoint with an H.323 ID alias of MeetingRoom1, an E.164 alias of 626262 and a SIP URI of MeetingRoom@domain.com. The entry also has H.235 and SIP credentials of ID meetingroom1 and password mypassword which are used during authentication.

H.323 registrations will look for the H.323 and H.235 attributes; SIP will look for the SIP attributes. Therefore if your endpoint is registering with just one protocol you do not need to include elements relating to the other.

Securing with TLS

The connection to the LDAP server can be encrypted by enabling Transport Level Security (TLS) on the connection. To do this you must create an X.509 certificate for the LDAP server to allow the VCS to verify the server's identity. Once the certificate has been created you will need to install the following three files associated with the certificate onto the LDAP server:

- The certificate for the LDAP server.
- The private key for the LDAP server.
- The certificate of the Certificate Authority (CA) that was used to sign the LDAP server's certificate.

All three files should be in PEM file format.

The LDAP server must be configured to use the certificate. To do this:

1. Edit /etc/openldap/slapd.conf and add the following three lines:

```
TLSCACertificateFile <path to CA certificate>
TLSCertificateFile <path to LDAP server certificate>
TLSCertificateKeyFile <path to LDAP private key>
```

The OpenLDAP daemon (slapd) must be restarted for the TLS settings to take effect.

To configure the VCS to use TLS on the connection to the LDAP server you must upload the CA's certificate as a trusted CA certificate. This can be done on the VCS by navigating to:

- Maintenance > Security.

The SIP URI in the ldif file must be prefixed by sip:.

For information about what happens when an alias is not in the LDAP database see the section Alias Origin Setting.

Command Reference - xConfiguration

Overview

The xConfiguration group of commands are used to set and change individual items of configuration. Each command is made up of a main element followed by one or more sub-elements.

The following pages list all the xConfiguration commands currently available on the VCS.

To set a particular item of configuration, type the command as shown. The valid values for each command are indicated in the angle brackets following each command; these are explained opposite.

To obtain information about the existing configuration on the VCS:

- type xConfiguration to return all current configuration settings for the VCS.
- type xConfiguration <element> to return all current configuration for that particular element and all its sub-elements.
- type xConfiguration <element> <sub-element> to return all current configuration for that group of sub-elements.

To obtain information about using each of the xConfiguration commands:

- type xConfiguration ? to return a list of all elements available under the xConfiguration command.
- type xConfiguration <element> ? to return all available sub-elements, along with the valuespace and description, and default values for each.
- type xConfiguration <element> <sub-element> ? to return all available sub-elements, along with the valuespace and description, and default values for each.

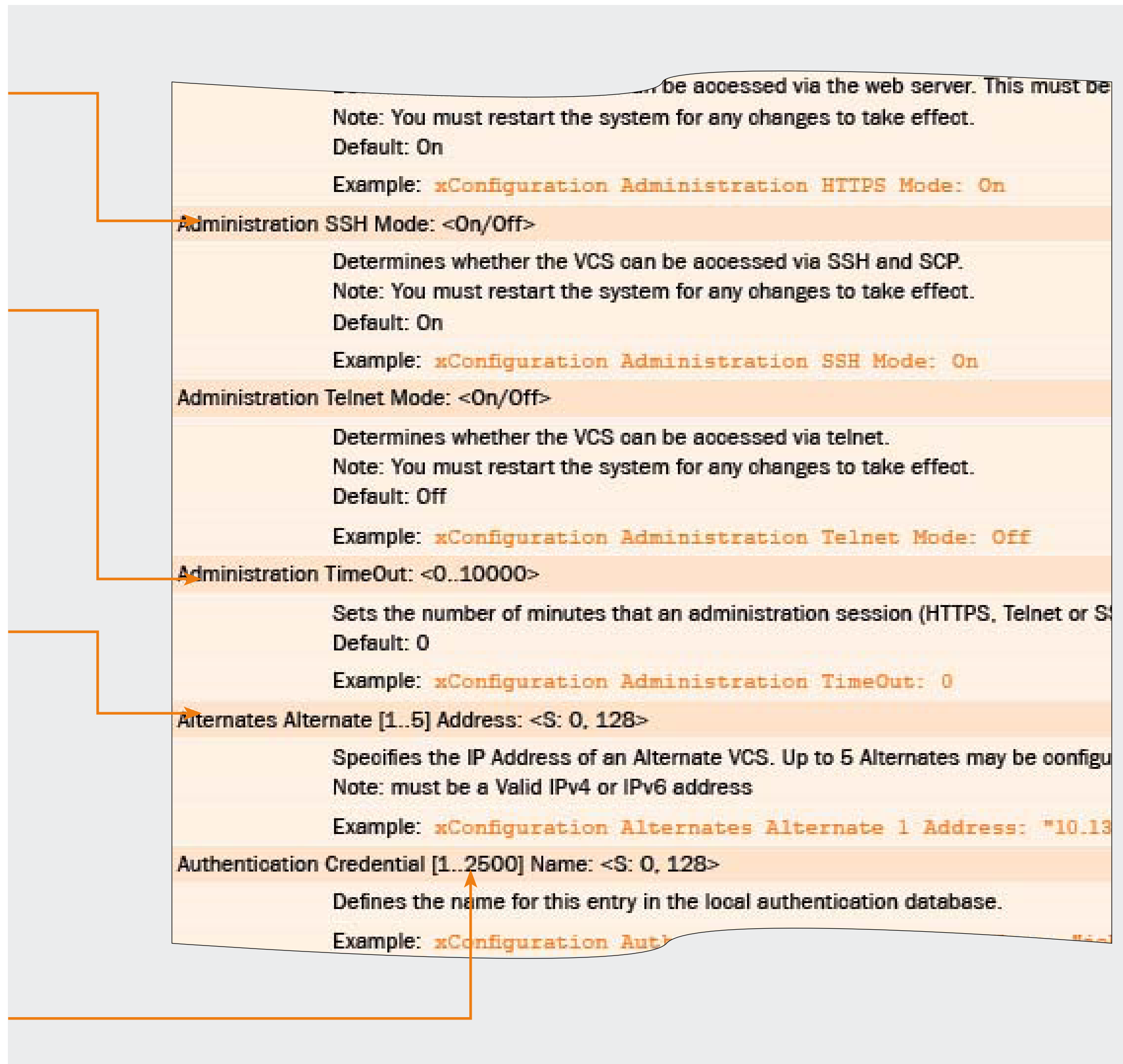
The valid values for this command are one of the options shown within the angle brackets.

The valid value for this command is an integer. The minimum and maximum values are shown within the angle brackets.

The valid value for this command is a string. The minimum and maximum number of characters is shown after the S.

When issuing this command, the string must be typed in double quotes.

Square brackets indicate that you can configure more than one of this particular item. Each item is assigned an index within the range shown.



Administration HTTP Mode: <On/Off>

Determines whether HTTP calls will be redirected to the HTTPS port.
On: calls will be redirected to HTTPS.
Off: no HTTP access will be available.
Note: You must restart the system for any changes to take effect.
Default: On

Example: `xConfiguration Administration HTTP Mode: On`

Administration HTTPS Mode: <On/Off>

Determines whether the VCS can be accessed via the web server. This must be On to enable both web interface and TMS access.
Note: You must restart the system for any changes to take effect.
Default: On

Example: `xConfiguration Administration HTTPS Mode: On`

Administration SSH Mode: <On/Off>

Determines whether the VCS can be accessed via SSH and SCP.
Note: You must restart the system for any changes to take effect.
Default: On

Example: `xConfiguration Administration SSH Mode: On`

Administration Telnet Mode: <On/Off>

Determines whether the VCS can be accessed via telnet.
Note: You must restart the system for any changes to take effect.
Default: Off

Example: `xConfiguration Administration Telnet Mode: Off`

Administration TimeOut: <0..10000>

Sets the number of minutes that an administration session (HTTPS, Telnet or SSH) may be inactive before the session is timed out. A value of 0 turns session time outs off.
Default: 0

Example: `xConfiguration Administration TimeOut: 0`

Alternates Peer [1..6] Address: <S: 0, 128>

Specifies the IP Address of one of the Peers in the Cluster to which this VCS belongs. A Cluster consists of up to 6 Peers, including the local VCS.
Note: Clusters should be managed via TMS.
Note: must be a Valid IPv4 or IPv6 address

Example: `xConfiguration Alternates 1 Peer Address: "10.13.0.2"`

Applications Presence Server Mode: <On/Off>

Enables and disables the SIMPLE Presence Server. Note: SIP Mode must also be enabled for the Presence Server to function.
Default: Off

Example: `Configuration Applications Presence Server Mode: On`

Applications Presence Server Publication ExpireDelta: <30..7200>

Specifies the maximum time (in seconds) within which a publisher must refresh its publication.
Default: 120

Example: `Configuration Applications Presence Server Publication ExpireDelta: 120`

Applications Presence Server Subscription ExpireDelta: <30..7200>

Specifies the maximum time (in seconds) within which a subscriber must refresh its subscription.
Default: 300

Example: `Configuration Applications Presence Server Subscription ExpireDelta:`

Applications Presence User Agent ExpireDelta: <1..65534>

Specifies the lifetime value (in seconds) the Presence User Agent will advertise in the PUBLISH messages it sends to the Presence Server. The User Agent will refresh its PUBLISH messages at 75% of this value (to keep them active). The Server may reduce this value in its responses.
Default: 3600

Example: `Configuration Applications Presence User Agent ExpireDelta: 3600`

Applications Presence User Agent Mode: <On/Off>

Enables and disables the SIMPLE Presence User Agent (PUA). The PUA provides presence information on behalf of registered endpoints. SIP Mode must also be enabled for the PUA to function.
Default: Off

Example: `Configuration Applications Presence User Agent Mode: Off`

Applications Presence User Agent RetryDelta: <1..65534>

Specifies the time (in seconds) after which the Presence User Agent will attempt to resend a PUBLISH to the Presence Server. This will occur if the original attempt failed due to resource issues or other transitory errors.
Default: 5

Example: `Configuration Applications Presence User Agent RetryDelta: 5`

Authentication Credential [1..2500] Name: <S: 0, 128>

Defines the name for this entry in the local authentication database.

Example: `xConfiguration Authentication Credential 1 Name: "john smith"`

Authentication Credential [1..2500] Password: <S: 0, 215>

Defines the password for this entry in the local authentication database. The maximum plaintext length is 128 characters, which will then be encrypted.

Example: `xConfiguration Authentication Credential 1 Password: "password123"`

Command Reference - xConfiguration

Authentication Database: <LocalDatabase/LDAPDatabase>

Selects between a local database and a remote LDAP repository for the storage of password information for authentication.
Default: LocalDatabase

Example: `xConfiguration Authentication Database: LocalDatabase`

Authentication LDAP AliasOrigin: <LDAP/Endpoint/Combined>

Determines which aliases (i.e. from the LDAP repository or the endpoint) should be used to register the endpoint.
Combined: the endpoint will be registered both with the aliases which it has presented and with those configured in the LDAP repository.
Default: LDAP

Example: `xConfiguration Authentication LDAP AliasOrigin: LDAP`

Authentication LDAP BaseDN: <S: 0, 255>

Specifies the Distinguished Name to use when connecting to an LDAP server.

Example: `xConfiguration Authentication LDAP BaseDN: "dc=example,dc=company,dc=com"`

Authentication Mode: <On/Off>

Determines whether systems attempting to communicate with the VCS must authenticate with it first.
Off: incoming messages are not authenticated.
On: for H.323, any credentials in the message are checked against the authentication database. The message is allowed if the credentials match, or of there are no credentials in the message. For SIP, any messages originating from an endpoint in a local domain will be authenticated.
Default: Off

Example: `xConfiguration Authentication Mode: Off`

Authentication Password: <S: 0, 215>

Specifies the password to be used by the VCS when authenticating with another system, including when your VCS is a traversal client connecting to a traversal server. The maximum plaintext length is 128 characters, which will then be encrypted.

Example: `xConfiguration Authentication Password: password123`

Authentication UserName: <S: 0, 128>

Specifies the username to be used by the VCS when authenticating with another system, including when your VCS is a traversal client connecting to a traversal server.

Example: `xConfiguration Authentication UserName: <S: 0, 128>`

Bandwidth Default: <64..2048>

Sets the bandwidth (in kbps) to be used on calls managed by the VCS in cases where no bandwidth has been specified by the endpoint.
Default: 384

Example: `xConfiguration Bandwidth Default: 384`

Bandwidth Downspeed PerCall Mode: <On/Off>

Determines whether or not the VCS will attempt to downspeed a call if there is insufficient per-call bandwidth available to fulfill the request.
On: the VCS will attempt to place the call at a lower bandwidth.
Off: the call will be rejected.
Default: On

Example: `xConfiguration Bandwidth Downspeed PerCall Mode: On`

Bandwidth Downspeed Total Mode: <On/Off>

Determines whether or not the VCS will attempt to downspeed a call if there is insufficient total bandwidth available to fulfill the request.
On: the VCS will attempt to place the call at a lower bandwidth.
Off: the call will be rejected.
Default: On

Example: `xConfiguration Bandwidth Downspeed Total Mode: On`

Bandwidth Link [1..600] Name: <S: 1, 50>

Assigns a name to this link.

Example: `xConfiguration Bandwidth Link 1 Name: "HQ to BranchOffice"`

Bandwidth Link [1..600] Node1 Name: <S: 0, 50>

Specifies the first zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node1 Name: "HQ"`

Bandwidth Link [1..600] Node2 Name: <S: 0, 50>

Specifies the second zone or subzone to which this link will be applied.

Example: `xConfiguration Bandwidth Link 1 Node2 Name: "BranchOffice"`

Bandwidth Link [1..600] Pipe1 Name: <S: 0, 50>

Specifies the first pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe1 Name: "512Kb ASDL"`

Bandwidth Link [1..600] Pipe2 Name: <S: 0, 50>

Specifies the second pipe to be associated with this link.

Example: `xConfiguration Bandwidth Link 1 Pipe2 Name: "2Gb Broadband"`

Bandwidth Pipe [1..100] Bandwidth PerCall Limit: <1..100000000>

If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call.
Default: 1920

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Limit: 256`

Bandwidth Pipe [1..100] Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is limiting the bandwidth of individual calls.
NoBandwidth: no bandwidth available. No calls can be made on this pipe.
Default: Unlimited

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth PerCall Mode: Limited`

Bandwidth Pipe [1..100] Bandwidth Total Limit: <1..100000000>

If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe.
Default: 500000

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Limit: 1024`

Bandwidth Pipe [1..100] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not this pipe is enforcing total bandwidth restrictions.
NoBandwidth: no bandwidth available. No calls can be made on this pipe.
Default: Unlimited

Example: `xConfiguration Bandwidth Pipe 1 Bandwidth Total Mode: Limited`

Bandwidth Pipe [1..100] Name: <S: 1, 50>

Assigns a name to this pipe.

Example: `xConfiguration Bandwidth Pipe 1 Name: "512Kb ASDL"`

Call Services CallsToUnknownIPAddresses: <Off/Direct/Indirect>

Determines the way in which the VCS will attempt to call systems which are not registered with it or one of its neighbors.
Direct: Allows an endpoint to make a call to an unknown IP Address without the VCS querying any neighbors. The call setup would occur just as it would if the far end were registered directly to the local system.
Indirect: Upon receiving a call to an unknown IP Address, the VCS will query its neighbors for the remote address and if permitted will route the call through the neighbor.
Off: Endpoints registered directly to the VCS may only call an IP Address of a system also registered directly to that VCS.
Default: Indirect

Example: `xConfiguration Call Services CallsToUnknownIPAddresses: Indirect`

Call Services Fallback Alias: <S: 0, 60>

Specifies the alias to which incoming calls are placed for calls where the IP Address or domain name of the VCS has been given but no callee alias has been specified.

Example: `xConfiguration Call Services Fallback Alias: "reception@example.com"`

Error Reports Mode: <On/Off>

Determines whether the VCS will automatically send details of application failures to a specified web service.
Note: You must restart the system for any changes to take effect.
Default: Off

Example: `xConfiguration Error Reports Mode: Off`

Error Reports URL: <S: 0, 128>

The URL of the web service to which error reports are sent.

Example: `xConfiguration Error Reports URL: "http://192.168.0.200/submitapplicationerror/"`

Ethernet [1..2] IP V4 Address: <IPAddr>

Specifies the IPv4 address of the specified LAN port.
Note: You must restart the system for any changes to take effect.
Default: 192.168.0.100

Example: `xConfiguration Ethernet 1 IP V4 Address: 192.168.10.10`

Ethernet [1..2] IP V4 SubnetMask: <IPAddr>

Specifies the IPv4 subnet mask of the specified LAN port.
Note: You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 IP V4 SubnetMask: 255.255.255.0`

Ethernet [1..2] IP V6 Address: <S: 0, 39>

Specifies the IPv6 address of the specified LAN port.
Note: You must restart the system for any changes to take effect

Example: `xConfiguration Ethernet 1 IP V6 Address: "2001:db8::1428:57ab"`

Ethernet [1..2] Speed: <Auto/10half/10full/100half/100full/1000full

Sets the speed of the Ethernet link from the specified LAN port. Use Auto to automatically configure the speed.
Note: You must restart the system for any changes to take effect.

Example: `xConfiguration Ethernet 1 Speed: Auto`

ExternalManager Address: <S: 0, 128>

Sets the IP Address or Fully Qualified Domain Name (FQDN) of the External Manager.

Example: `xConfiguration ExternalManager Address: 192.168.0.0`

ExternalManager Path: <S: 0, 255>

Sets the URL of the External Manager.
Default: tms/public/external/management/SystemManagementService.asmx

Example: `xConfiguration ExternalManager Path: "tms/public/external/management/SystemManagementService.asmx"`

H323 Gatekeeper AutoDiscovery Mode: <On/Off>

Determines whether or not the VCS responds to gatekeeper discovery requests from endpoints.
Default: On

Example: `xConfiguration H323 Gatekeeper AutoDiscovery Mode: On`

Command Reference - xConfiguration

H323 Gatekeeper CallSignaling PortRange End: <1024..65534>

Specifies the upper port in the range to be used by calls once they are established.
Default: 19999

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999`

H323 Gatekeeper CallSignaling PortRange Start: <1024..65534>

Specifies the lower port in the range to be used by calls once they are established.
Default: 15000

Example: `xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000`

H323 Gatekeeper CallSignaling TCP Port: <1024..65534>

Specifies the port that listens for H.323 call signaling.
Default: 1720

Example: `xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720`

H323 Gatekeeper CallTimeToLive: <60..65534>

Specifies the interval (in seconds) at which the VCS polls the endpoints in a call to verify that they are still in the call.
Default: 120

Example: `xConfiguration H323 Gatekeeper CallTimeToLive: 120`

H323 Gatekeeper Registration ConflictMode: <Reject/Overwrite>

Determines how the system will behave if an endpoint attempts to register an alias currently registered from another IP Address.
Reject: denies the registration.
Overwrite: deletes the original registration and replaces it with the new registration.
Default: Reject

Example: `xConfiguration H323 Gatekeeper Registration ConflictMode: Reject`

H323 Gatekeeper Registration UDP Port: <1024..65534>

Specifies the port to be used for H.323 UDP registrations.
Default: 1719

Example: `xConfiguration H323 Gatekeeper Registration UDP Port: 1719`

H323 Gatekeeper TimeToLive: <60..65534>

Specifies the interval (in seconds) at which an H.323 endpoint must re-register with the VCS in order to confirm that it is still functioning.
Default: 1800

Example: `xConfiguration H323 Gatekeeper TimeToLive: 1800`

H323 Mode: <On/Off>

Determines whether or not the VCS will provide H.323 gatekeeper functionality.
Default: On

Example: `xConfiguration H323 Mode: On`

Interworking Encryption Mode: <Auto/Off>

Determines whether or not the VCS will allow encrypted calls between SIP and H.323 endpoints.
Off: interworked calls will never be encrypted.
Auto: interworked calls will be encrypted if the endpoints request it.
Default: Auto

Example: `xConfiguration Interworking Encryption Mode: Auto`

Interworking Mode: <On/Off/RegisteredOnly>

Determines whether or not the VCS will act as a gateway between SIP and H.323 calls.
Off: the VCS will not act as a SIP-H.323 gateway.
RegisteredOnly: the VCS will act as a SIP-H.323 gateway but only if at least one of the endpoints is locally registered.
On: the VCS will act as SIP-H.323 gateway regardless of whether the endpoints are locally registered.
Default: RegisteredOnly

Example: `xConfiguration Interworking Mode: RegisteredOnly`

IP DNS Domain Name: <S: 0, 128>

Specifies the name to be appended to the host name before a query to the DNS server is executed. Used only when attempting to resolve a domain name which is not fully qualified for NTP, LDAP, External Manager and Log servers.

Example: `xConfiguration IP DNS Domain Name: "example.net"`

IP DNS Server [1..5] Address: <S: 0, 39>

Sets the IP Address of up to 5 DNS servers to be used when resolving domain names.

Example: `xConfiguration IP DNS Server 1 Address: "192.168.12.0"`

IP Gateway: <IPAddr>

Specifies the IPv4 gateway of the VCS.
Note: You must restart the system for any changes to take effect.
Default: 127.0.0.1

Example: `xConfiguration IP Gateway: 192.168.127.0`

IP Route [1..50] Address: <S: 0, 39>

Specifies an IP Address used in conjunction with the Prefix Length to determine the network to which this route applies.

Example: `xConfiguration IP Route 1 Address: "128.168.0.0"`

IP Route [1..50] Gateway: <S: 0, 39>

Specifies the IP Address of the Gateway for this route.

Example: `xConfiguration IP Route 1 Gateway: "192.168.0.0"`

IP Route [1..50] Interface: <Auto/LAN1/LAN2>

Specifies the LAN interface to use for this route. Auto: The VCS will select the most appropriate interface to use.
Default: Auto

Example: `xConfiguration IP Route 1 Interface: Auto`

IP Route [1..50] PrefixLength: <0..128>

Specifies the number of bits of the IP Address which must match when determining the network to which this route applies.

Example: `xConfiguration IP Route 1 PrefixLength: 16`

IP V6 Gateway: <S: 0, 39>

Specifies the IPv6 gateway of the VCS. Note: You must restart the system for any changes to take effect.

Example: `xConfiguration IP V6 Gateway: "3dda:80bb:6::9:144"`

IPProtocol: <Both/IPv4/IPv6>

Selects whether the VCS is operating in IPv4, IPv6 or dual stack mode.
Note: You must restart the system for any changes to take effect.
Default: IPv4

Example: `xConfiguration IPProtocol: IPv4`

LDAP Encryption: <Off/TLS>

Sets the encryption to be used for the connection to the LDAP server.
Off: no encryption is used.
TLS: TLS encryption is used.
Default: Off

Example: `xConfiguration LDAP Encryption: Off`

LDAP Password: <S: 0, 122>

Sets the password to be used when binding to the LDAP server. The maximum plaintext length is 60 characters, which will then be encrypted.

Example: `xConfiguration LDAP Password: "password123"`

LDAP Server Address: <S: 0, 128>

Sets the IP Address or Fully Qualified Domain Name (FQDN) of the LDAP server to be used when making LDAP queries.

Example: `xConfiguration LDAP Server Address: "ldap.server.example.com"`

LDAP Server Port: <1..65534>

Sets the IP port of the LDAP server to be used when making LDAP queries.
Default: 389

Example: `xConfiguration LDAP Server Port: 389`

LDAP UserDN: <S: 0, 255>

Sets the user distinguished name to be used when binding to the LDAP server.

Example: `xConfiguration LDAP UserDN: "User123"`

Log Level: <1..4>

Controls the granularity of event logging. 1 is the least verbose, 4 the most.
Note: this setting is not retrospective; it will determine which events are written to the event log from now onwards.
Default: 1

Example: `xConfiguration Log Level: 1`

Log Server Address: <S: 0, 128>

Specifies the IP Address or Fully Qualified Domain Name (FQDN) of the remote syslog server to which the log will be written. This server must support the BSD syslog protocol. It cannot be another VCS.

Example: `xConfiguration Log Server Address: "syslog.server.example.com"`

NTP Address: <S: 0, 128>

Sets the IP Address or Fully Qualified Domain Name (FQDN) of the NTP server to be used when synchronizing system time.

Example: `xConfiguration NTP Address: "ntp.server.example.com"`

Option [1..64] Key: <S: 0, 90>

Specifies the option key of your software option. These are added to the VCS in order to add extra functionality, such as increasing the VCS's capacity. Contact your TANDBERG representative for further information.

Example: `xConfiguration Option 1 Key: "1X4757T5-1-60BAD5CD"`

Policy AdministratorPolicy Mode: <On/Off>

Enables and disables use of Administrator Policy.
Default: Off

Example: `xConfiguration Policy AdministratorPolicy Mode: Off`

Policy UserPolicy Mode: <Off/Local/Remote>

Determines the User Policy Manager usage and location.
Off: User Policy Manager is not used.
Local: the on-box User Policy Manager is used.
Remote: the off-box User Policy Manager is used.
Default: Local

Example: `xConfiguration Policy UserPolicy Mode: Local`

Policy UserPolicy Server Address: <S: 0, 128>

Specifies the IP Address or Fully Qualified Domain Name (FQDN) of the remote User Policy Manager.

Example: `xConfiguration Policy UserPolicy Server Address: "userpolicy.server.example.com"`

Policy UserPolicy Server Password: <S: 0, 82>

Specifies the password used by the VCS to log in and query the remote User Policy Manager. The maximum plaintext length is 30 characters, which will then be encrypted.

Example: `xConfiguration Policy UserPolicy Server Password: "password123"`

Policy UserPolicy Server Path: <S: 0, 255>

Specifies the URL of the remote User Policy Manager.
Default: otimgr/query.php

Example: `xConfiguration Policy UserPolicy Server Path: otimgr/query.php`

Policy UserPolicy Server Protocol: <HTTP/HTTPS>

Specifies the protocol used to connect to the remote User Policy Manager.
Default: HTTP

Example: `xConfiguration Policy UserPolicy Server Protocol: HTTP`

Policy UserPolicy Server UserName: <S: 0, 30>

Specifies the user name used by the VCS to log in and query the remote User Policy Manager.

Example: `xConfiguration Policy UserPolicy Server UserName: "User123"`

Registration AllowList [1..2500] Pattern String: <S: 0, 60>

Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.

Example: `xConfiguration Registration AllowList 1 Pattern String: "john.smith@example.com"`

Registration AllowList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly.
Exact: the string must match the alias character for character.
Prefix: the string must appear at the beginning of the alias.
Suffix: the string must appear at the end of the alias.
Regex: the string will be treated as a regular expression.
Default: Exact

Example: `xConfiguration Registration AllowList 1 Pattern Type: Exact`

Registration DenyList [1..2500] Pattern String: <S: 0, 60>

Specifies an entry to be added to the Deny List. If one of an endpoint’s aliases matches one of the patterns in the Deny List, the registration will not be permitted.

Example: `xConfiguration Registration DenyList 1 Pattern String: "john.jones@example.com"`

Registration DenyList [1..2500] Pattern Type: <Exact/Prefix/Suffix/Regex>

Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly.
Exact: the string must match the alias character for character.
Prefix: the string must appear at the beginning of the alias.
Suffix: the string must appear at the end of the alias.
Regex: the string will be treated as a regular expression.
Default: Exact

Example: `xConfiguration Registration DenyList 1 Pattern Type: Exact`

Registration RestrictionPolicy: <None/AllowList/DenyList>

Specifies the policy to be used when determining which endpoints may register with the system.
None: No restriction.
AllowList: Only endpoints attempting to register with an alias listed on the Allow List may register.
DenyList: All endpoints, except those attempting to register with an alias listed on the Deny List, may register.
Default: None

Example: `xConfiguration Registration RestrictionPolicy: None`

SIP Domains Domain [1..20] Name: <S: 0, 128>

Specifies a domain for which this VCS is authoritative. The VCS will act as a SIP Registrar and Presence Server for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain.

Example: `xConfiguration SIP Domains Domain 1 Name: "example.com"`

SIP Loop Detect Mode: <On/Off>

Specifies whether SIP loop detection is performed.
Default: On

Example: `Configuration SIP Loop Detect Mode: On`

SIP Mode: <On/Off>

Determines whether or not the VCS will provide SIP registrar and SIP proxy functionality. This mode must be enabled in order to use either the Presence Server or the Presence User Agent.
Default: On

Example: `xConfiguration SIP Mode: On`

SIP Registration ExpireDelta: <30..7200>

Specifies the period (in seconds) within which a SIP endpoint must re-register with the VCS to prevent its registration expiring.
Default: 60

Example: `xConfiguration SIP Registration ExpireDelta: 60`

SIP Registration Proxy Mode: <Off/ProxyToKnownOnly/ProxyToAny>

Specifies how proxied registrations should be handled.
Off: Registration requests will not be proxied.
ProxyToKnownOnly: Registration requests will be proxied to neighbors only.
ProxyToAny: Registration requests will be proxied in accordance with the VCS's existing call processing rules.
Default: Off

Example: `xConfiguration SIP Registration Proxy Mode: Off`

SIP TCP Mode: <On/Off>

Determines whether incoming SIP calls using the TCP protocol will be allowed.
Default: On

Example: `xConfiguration SIP TCP Mode: On`

SIP TCP Outbound Port End: <1024..65534>

Specifies the upper port in the range to be used by outbound TCP/TLS SIP connections.
Default: 29999

Example: `xConfiguration SIP TCP Outbound Port End: 29999`

SIP TCP Outbound Port Start: <1024..65534>

Specifies the lower port in the range to be used by outbound TCP/TLS SIP connections.
Default: 25000

Example: `xConfiguration SIP TCP Outbound Port Start: 25000`

SIP TCP Port: <1024..65534>

Specifies the listening port for incoming SIP TCP calls.
Default: 5060

Example: `xConfiguration SIP TCP Port: 5060`

SIP TLS Mode: <On/Off>

Determines whether incoming SIP calls using the TLS protocol will be allowed.
Default: On

Example: `xConfiguration SIP TLS Mode: On`

SIP TLS Port: <1024..65534>

Specifies the listening port for incoming SIP TLS calls.
Default: 5061

Example: `xConfiguration SIP TLS Port: 5061`

SIP UDP Mode: <On/Off>

Determines whether incoming SIP calls using the UDP protocol will be allowed.
Default: On

Example: `xConfiguration SIP UDP Mode: On`

SIP UDP Port: <1024..65534>

Specifies the listening port for incoming SIP UDP calls.
Default: 5060

Example: `xConfiguration SIP UDP Port: 5060`

SNMP CommunityName: <S: 0, 16>

Sets the VCS's SNMP community name.
Default: public

Example: `xConfiguration SNMP CommunityName: "public"`

SNMP Mode: <On/Off>

Enables or disables SNMP support.
Note: You must restart the system for any changes to take effect.
Default: Off

Example: `xConfiguration SNMP Mode: On`

SNMP SystemContact: <S: 0, 70>

Specifies the name of the person who can be contacted regarding issues with the VCS.

Example: `xConfiguration SNMP SystemContact: "John Smith"`

SNMP SystemLocation: <S: 0, 70>

Specifies the physical location of the VCS.

Example: `xConfiguration SNMP SystemLocation: "Server Room 128"`

SystemUnit AdminAccount [1..15] Access : <Account Disabled/Read Only/Read Write>	
	Defines the Access level of an administration user who can login to the VCS Web interface. The Access determines whether the user can access the VCS, and if so whether they can change the configuration or just view it.
	Example: `xConfiguration SystemUnit AdminAccount [1..15] Access : Read Only`
SystemUnit AdminAccount [1..15] Name : <S:0..25>	
	Defines the name of an administration user who can login to the VCS Web interface.
	Example: `xConfiguration SystemUnit AdminAccount [1..15] Name : "guest"`
SystemUnit AdminAccount [1..15] Password : <S:0..65>	
	Defines the password of an administration user who can login to the VCS Web interface. The maximum plaintext length is 16 characters, which will then be encrypted.
	Example: `xConfiguration SystemUnit AdminAccount [1..15] Password : "password123"`
SystemUnit Name: <S:, 0, 50>	
	Defines the name of the VCS. Choose a name that uniquely identifies the system.
	Example: `xConfiguration SystemUnit Name: "Oslo HQ VCS"`
SystemUnit Password: <S: 0, 65>	
	Defines the password for the default 'admin' account. This account is used to log in to the VCS via Telnet, HTTP(S), SSH, SCP, and on the serial port. The maximum plaintext length is 16 characters, which will then be encrypted.
	Example: `xConfiguration SystemUnit Password: "password123"`
TimeZone Name: <S: 0, 64>	
	Sets the local time zone of the VCS. Time zone names follow the POSIX naming convention e.g. Europe/London or America/New_York. Default: GMT
	Example: `xConfiguration TimeZone Name: "GMT"`
Transform [1..100] Pattern Behavior: <Strip/Replace>	
	Determines how the matched part of the alias will be modified. Strip: the matching prefix or suffix will removed from the alias. Replace: the matching part of the alias will be substituted with the text in the Pattern Replace string.
	Example: `xConfiguration Transform 1 Pattern Behavior: Replace`
Transform [1..100] Pattern Replace: <S: 0, 60>	
	(Applies only if pattern behavior is set to Replace.) Specifies the string to be used as a substitution for the part of the alias that matched the pattern.
	Example: `xConfiguration Transform 1 Pattern Replace: "example.com"`
Transform [1..100] Pattern String: <S: 0, 60>	
	Specifies the pattern against which the alias is compared.
	Example: `xConfiguration Transform 1 Pattern String: "example.net"`

Transform [1..100] Pattern Type: <Exact/Prefix/Suffix/Regex>

Determines the way in which the string must match the alias.
Exact: the string must match the alias character for character.
Prefix: the string must appear at the beginning of the alias.
Suffix: the string must appear at the end of the alias.
Regex: the string will be treated as a regular expression.

Example: `xConfiguration Transform 1 Pattern Type: Suffix`

Transform [1..100] Priority: <1..65534>

Assigns a priority to the specified transform. Transforms are applied in order of priority, and the priority must be unique for each transform.

Example: `xConfiguration Transform 1 Priority: 10`

Traversal Media Port End: <1025..65533>

For traversal calls (i.e. where the VCS is taking the media as well as the signaling), specifies the upper port in the range to be used for the media. Ports are allocated from this range in pairs, the first of each being even. Therefore the range must end with an odd number.
Default: 51199

Example: `xConfiguration Traversal Media Port End: 51199`

Traversal Media Port Start: <1024..65532>

For traversal calls (i.e. where the VCS is taking the media as well as the signaling), specifies the lower port in the range to be used for the media. Ports are allocated from this range in pairs, the first of each being even. Therefore the range must start with an even number.
Default: 50000

Example: `xConfiguration Traversal Media Port Start: 50000`

Traversal Server H323 Assent CallSignaling Port: <1024..65534>

Specifies the port on the VCS to be used for Assent signaling.
Default: 2776

Example: `xConfiguration Traversal Server H323 Assent CallSignaling Port: 2777`

Traversal Server H323 H46018 CallSignaling Port: <1024..65534>

Specifies the port on the VCS to be used for H460.18 signaling.
Default: 2777

Example: `Traversal Server H323 H46018 CallSignaling Port: 2777`

Traversal Server Media Demultiplexing RTCP Port: <1024..65534>

Specifies the port on the VCS to be used for demultiplexing RTCP media. Note: You must restart the system for any changes to take effect.
Default: 2777

Example: `xConfiguration Traversal Server Media Demultiplexing RTCP Port: 2777`

Traversal Server Media Demultiplexing RTP Port: <1024..65534>

Specifies the port on the VCS to be used for demultiplexing RTP media. Note: You must restart the system for any changes to take effect.
Default: 2776

Example: `xConfiguration Traversal Server Media Demultiplexing RTP Port: 2776`

Traversal Server STUN Discovery Mode: <On/Off>

Determines whether the VCS will offer STUN discovery services to traversal clients.
Default: On

Example: `xConfiguration Traversal Server STUN Discovery Mode: On`

Traversal Server STUN Discovery Port: <1024..65534>

Specifies the port to be used for STUN discovery services.
Default: 3478

Example: `xConfiguration Traversal Server STUN Discovery Port: 4678`

Traversal Server STUN Relay Media Port End: <1024..65534>

Specifies the upper port in the range to be used for STUN media relay.
Default: 61200

Example: `xConfiguration Traversal Server STUN Relay Media Port End: 61200`

Traversal Server STUN Relay Media Port Start: <1024..65534>

Specifies the lower port in the range to be used for STUN media relay.
Default: 60000

Example: `xConfiguration Traversal Server STUN Relay Media Port Start: 60000`

Traversal Server STUN Relay Mode: <On/Off>

Determines whether the VCS will offer STUN relay services to traversal clients.
Default: On

Example: `xConfiguration Traversal Server STUN Relay Mode: On`

Traversal Server STUN Relay Port: <1024..65534>

Specifies the listening port for STUN relay requests.
Default: 4678

Example: `Traversal Server STUN Relay Port: 4678`

Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) for any one call to or from an endpoint in the Default Subzone (applies only if Mode is set to Limited).
Default: 1920

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Limit: 1920`

Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in the Default Subzone.
NoBandwidth: no bandwidth available. No calls can be made to or from the Default Subzone.
Default: Unlimited

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode: Limited`

Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) for any one call between two endpoints within the Default Subzone (applies only if Mode is set to Limited).
Default: 1920

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Limit: 1920`

Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call between two endpoints within the Default Subzone.
NoBandwidth: no bandwidth available. No calls can be made within the Default Subzone.
Default: Unlimited

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode: Limited`

Zones LocalZone DefaultSubZone Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of the Default Subzone (applies only if Mode is set to Limited).
Default: 500000

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Limit: 500000`

Zones LocalZone DefaultSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time.
NoBandwidth: no bandwidth available. No calls can be made to, from, or within the Default Subzone.
Default: Unlimited

Example: `xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Limited`

Zones LocalZone Match [1..5] Mode : <AlwaysMatch/PatternMatch/Disabled>

Determines if and when a query will be sent to the Local Zone.
AlwaysMatch: the zone will always be queried.
PatternMatch: the zone will only be queried if the alias queried for matches the corresponding pattern.
Disabled: the zone will never be queried.
Default: AlwaysMatch (Match 1); Disabled (Matches 2-5)

Example: `xConfiguration Zones LocalZone Match [1..5] Mode : PatternMatch`

Zones LocalZone Match [1..5] Pattern Behavior : <Strip/Leave/Replace>

Determines how the matched part of the alias will be modified.
Strip: the matching prefix or suffix will removed from the alias.
Replace: the matching part of the alias will be substituted with the text in the Replace string.
Leave: the alias will not be modified.

Example: `xConfiguration Zones LocalZone Match [1..5] Pattern Behavior : replace`

Zones LocalZone Match [1..5] Pattern Replace : <S:0..60>

(Applies only if pattern behavior is set to Replace.) Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Example: `xConfiguration Zones LocalZone Match [1..5] Pattern Replace : "@example.com"`

Zones LocalZone Match [1..5] Pattern String : <S:0..60>

Specifies the pattern against which the alias is compared.

Example: `xConfiguration Zones LocalZone Match [1..5] Pattern String : "@example.net"`

Zones LocalZone Match [1..5] Pattern Type : <Exact/Prefix/Suffix/Regex>

Determines the way in which the string must match the alias.
Exact: the string must match the alias character for character.
Prefix: the string must appear at the beginning of the alias.
Suffix: the string must appear at the end of the alias.
Regex: the string will be treated as a regular expression.

Example: `xConfiguration Zones LocalZone Match [1..5] Pattern Type : suffix`

Zones LocalZone Match [1..5] Priority : <1..65534>

Determines the order in which the zone will be sent a search request. Zones with priority 1 matches are searched first, followed by priority 2, and so on.
Default: 50

Example: `xConfiguration Zones LocalZone Match [1..5] Priority : 100`

Zones LocalZone SubZone [1..100] Bandwidth PerCall Inter Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if Mode is set to Limited).
Default: 1920

Example: `xConfiguration Zones LocalZone SubZone 1 Bandwidth PerCall Inter Limit: 1920`

Zones LocalZone SubZone [1..100] Bandwidth PerCall Inter Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone.
NoBandwidth: no bandwidth available. No calls can be made to or from this subzone.
Default: Unlimited

Example: `xConfiguration Zones LocalZone SubZone 1 Bandwidth PerCall Inter Mode: Limited`

Zones LocalZone SubZone [1..100] Bandwidth PerCall Intra Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) for any one call between two endpoints within this subzone (applies only if Mode is set to Limited).
Default: 1920

Example: `Zones LocalZone SubZone 1 Bandwidth PerCall Intra Limit: 1920`

Zones LocalZone SubZone [1..100] Bandwidth PerCall Intra Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone.
NoBandwidth: no bandwidth available. No calls can be made within this subzone.
Default: Unlimited

Example: `xConfiguration Zones LocalZone SubZone 1 Bandwidth PerCall Intra Mode: Limited`

Zones LocalZone SubZone [1..100] Bandwidth Total Limit: <1..100000000>

Sets the total bandwidth limit (in kbps) of this subzone (applies only if Mode is set to Limited).
Default: 500000

Example: `xConfiguration Zones LocalZone SubZone 1 Bandwidth Total Limit: 500000`

Zones LocalZone SubZone [1..100] Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether this subzone has a limit on the total bandwidth of calls being used by its endpoints at any one time.
NoBandwidth: no bandwidth available. No calls can be made to, from, or within this subzone.
Default: Unlimited

Example: `xConfiguration Zones LocalZone SubZone 1 Bandwidth Total Mode: Limited`

Zones LocalZone SubZone [1..100] Name: <S: 1, 50>

Assigns a name to this subzone.

Example: `xConfiguration Zones LocalZone SubZone 1 Name: "BranchOffice"`

Zones LocalZone SubZone [1..100] Subnet [1..5] IP Address: <S: 0, 39>

Specifies an IP Address used (in conjunction with the IP Prefix Length) to identify a subnet to be assigned to this subzone.
Default: 0.0.0.0

Example: `xConfiguration Zones LocalZone SubZone 1 Subnet 1 IP Address: 192.168.0.0`

Zones LocalZone SubZone [1..100] Subnet [1..5] IP PrefixLength: <0..128>

Specifies the number of bits of the Subnet IP Address which must match for an IP Address to belong in this subzone.
Default: 32

Example: `xConfiguration Zones LocalZone SubZone 1 Subnet 1 IP PrefixLength: 64`

Zones LocalZone Traversal H323 Assent Mode: <On/Off>

Determines whether or not H.323 calls using Assent mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the VCS.
Default: On

Example: `xConfiguration Zones LocalZone Traversal H323 Assent Mode: On`

Zones LocalZone Traversal H323 H46018 Mode: <On/Off>

Determines whether or not H.323 calls using H460.18 mode for firewall traversal will be allowed. Applies to traversal-enabled endpoints registered directly with the VCS.
Default: On

Example: `xConfiguration Zones LocalZone Traversal H323 H46018 Mode: On`

Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: <On/Off>

Determines whether the VCS will operate in Demultiplexing mode for calls from traversal-enabled endpoints registered directly with it.
On: allows use of the same two ports for all calls.
Off: Each call will use a separate pair of ports for media.
Default: Off

Example: `xConfiguration Zones LocalZone Traversal H323 H46019 Demultiplexing Mode: Off`

Zones LocalZone Traversal H323 Preference: <Assent/H46018>

If an endpoint that is registered directly with the VCS supports both Assent and H460.18 protocols, this setting determines which the VCS uses.
Default: Assent

Example: `xConfiguration Zones LocalZone Traversal H323 Preference: Assent`

Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
Default: 20

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe KeepAliveInterval: 20`

Zones LocalZone Traversal H323 TCPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a TCP probe to the VCS.
Default: 5

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryCount: 5`

Zones LocalZone Traversal H323 TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a TCP probe to the VCS.
Default: 2

Example: `xConfiguration Zones LocalZone Traversal H323 TCPProbe RetryInterval: 2`

Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which a traversal-enabled endpoint registered directly with the VCS will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
Default: 20

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe KeepAliveInterval: 20`

Zones LocalZone Traversal H323 UDPProbe RetryCount: <1..65534>

Sets the number of times traversal-enabled endpoints registered directly with the VCS will attempt to send a UDP probe to the VCS.
Default: 5

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryCount: 5`

Zones LocalZone Traversal H323 UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which traversal-enabled endpoints registered directly with the VCS will send a UDP probe to the VCS.
Default: 2

Example: `xConfiguration Zones LocalZone Traversal H323 UDPProbe RetryInterval: 2`

Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: <1..100000000>

Specifies the bandwidth limit (in kbps) applied to any one traversal call being handled by the VCS (applies only if Mode is set to Limited).
Default: 1920

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Limit: 1920`

Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: <Limited/Unlimited/NoBandwidth>

Determines whether there is a limit on the bandwidth of any one traversal call being handled by the VCS.
NoBandwidth: no bandwidth available. No traversal calls can be made.
Default: Unlimited

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode: Limited`

Zones LocalZone TraversalSubZone Bandwidth Total Limit: <1..100000000>

Specifies the total bandwidth (in kbps) allowed for all traversal calls being handled by the VCS (applies only if Mode is set to Limited).
Default: 500000

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Limit: 500000`

Zones LocalZone TraversalSubZone Bandwidth Total Mode: <Limited/Unlimited/NoBandwidth>

Determines whether or not there is a limit to the total bandwidth of all traversal calls being handled by the VCS.
NoBandwidth: no bandwidth available. No traversal calls can be made.
Default: Unlimited

Example: `xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Limited`

Zones Zone [1..200] DNS Interworking SIP Audio DefaultCodec : <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AALCD_48/AALCD_56/AALCD_64/AMR>

Specifies which audio codec to use when empty INVITEs are not allowed.
Default: G711u

Example: `xConfiguration Zones Zone [1..200] DNS Interworking SIP Audio DefaultCodec : G711u`

Zones Zone [1..200] DNS Interworking SIP EmptyInviteAllowed : <On/Off>

Determines whether the VCS will generate a SIP INVITE message with no SDP to send to this zone. INVITES with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323.
On: SIP INVITEs with no SDP will be generated and sent to this neighbor.
Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor.
Default: On

Example: `xConfiguration Zones Zone [1..200] DNS Interworking SIP EmptyInviteAllowed : On`

Zones Zone [1..200] DNS Interworking SIP Video DefaultBitrate : <64..2048>

Specifies which video bitrate to use when empty INVITEs are not allowed.
Default: 384

Example: `xConfiguration Zones Zone [1..200] DNS Interworking SIP Video DefaultBitrate : 384`

Zones Zone [1..200] DNS Interworking SIP Video DefaultCodec : <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed.
Default: H263

Example: `xConfiguration Zones Zone [1..200] DNS Interworking SIP Video DefaultCodec : H263`

Zones Zone [1..200] DNS Interworking SIP Video DefaultResolution : <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed.
Default: CIF

Example: `xConfiguration Zones Zone [1..200] DNS Interworking SIP Video DefaultResolution : CIF`

Zones Zone [1..200] DNS SIP SearchAutoResponse : <On/Off>

Determines what happens when the VCS receives a SIP search that originated as an H.323 search, destined for this zone.
Off: a SIP OPTION message will be sent to the zone.
On: searches will be responded to automatically, without being forwarded to the zone..
Default: Off.

Example: `xConfiguration Zones Zone [1..200] DNS SIP SearchAutoResponse :`

Zones Zone [1..200] ENUM DNSSuffix: <S: 0, 128>

Specifies the DNS zone to be appended to the transformed E.164 number to create an ENUM host name which this zone is then queried for.

Example: `xConfiguration Zones Zone 1 ENUM DNSSuffix: "e164.arpa"`

Zones Zone [1..200] H323 Mode: <On/Off>

Determines whether H.323 calls will be allowed to and from this zone.
Default: On

Example: `xConfiguration Zones Zone 1 H323 Mode: On`

Zones Zone [1..200] HopCount: <1..255>

Specifies the hop count to be used when sending an alias search request to this zone. Note: if the search request was received from another zone and already has a hop count assigned, the lower of the two values will be used.
Default: 15

Example: `xConfiguration Zones Zone 1 HopCount: 15`

Zones Zone [1..200] Match [1..5] Mode: <AlwaysMatch/PatternMatch/Disabled>

Determines if and when a query will be sent to this zone.
AlwaysMatch: the zone will always be queried.
PatternMatch: the zone will only be queried if the alias queried for matches the corresponding pattern.
Disabled: the zone will never be queried.
Default: AlwaysMatch (Match 1) Disabled (Matches 2-5)

Example: `xConfiguration Zones Zone 1 Match 1 Mode: PatternMatch`

Zones Zone [1..200] Match [1..5] Pattern Behavior: <Strip/Leave/Replace>

(Applies only if the Match mode is Pattern Match.) Determines whether the matched part of the alias should be modified before an LRQ is sent to this zone.
Leave: the alias will be unmodified.
Strip: the matching prefix or suffix will be removed from the alias.
Replace: the matching part of the alias will be substituted with the text in the Replace string.
Default: Leave

Example: `xConfiguration Zones Zone 1 Match 1 Pattern Behavior: Replace`

Zones Zone [1..200] Match [1..5] Pattern Replace: <S: 0, 60>

(Applies only if the Pattern Behavior is Replace.) Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Example: `xConfiguration Zones Zone 1 Match 1 Pattern Replace: "example.com"`

Zones Zone [1..200] Match [1..5] Pattern String: <S: 0, 60>

(Applies only if the Match mode is Pattern Match.) Specifies the pattern against which the alias is compared.

Example: `xConfiguration Zones Zone 1 Match 1 Pattern String: "example.net"`

Zones Zone [1..200] Match [1..5] Pattern Type: <Exact/Prefix/Suffix/Regex>

(Applies only if the Match mode is Match.) Determines the way in which the string must match the alias.
Exact: the string must match the alias character for character.
Prefix: the string must appear at the beginning of the alias.
Suffix: the string must appear at the end of the alias.
Regex: the string will be treated as a regular expression.
Default: Prefix

Example: `xConfiguration Zones Zone 1 Match 1 Pattern Type: Suffix`

Zones Zone [1..200] Match [1..5] Priority: <1..65534>

Determines the order in which the zone will be sent a search request. Zones with priority 1 matches are searched first, followed by priority 2, and so on.
Default: 100

Example: `xConfiguration Zones Zone 1 Match 1 Priority: 100`

Zones Zone [1..200] Name: <S: 1, 50>

Assigns a name to this zone.

Example: `xConfiguration Zones Zone 1 Name: "UK Sales Office"`

Zones Zone [1..200] Neighbor H323 Port: <1024..65534>

Specifies the port on the neighbor to be used for H.323 calls to and from this VCS.
Default: 1719

Example: `xConfiguration Zones Zone 1 Neighbor H323 Port: 1719`

Zones Zone [1..200] Neighbor Interworking SIP Audio DefaultCodec : <G711u/G711a/G722_48/G722_56/G722_64/G722_1_16/G722_1_24/G722_1_32/G722_1_48/G723_1/G728/G729/AALCD_48/AALCD_56/AALCD_64/AMR>

Specifies which audio codec to use when empty INVITEs are not allowed.
Default: G711u

Example: `xConfiguration Zones Zone 1 Neighbor Interworking SIP Audio DefaultCodec : G711u`

Zones Zone [1..200] Neighbor Interworking SIP EmptyInviteAllowed : <On/Off>

Determines whether the VCS will generate a SIP INVITE message with no SDP to send to this zone. INVITES with no SDP mean that the destination device is asked to initiate the codec selection, and are used when the call has been interworked locally from H.323.
On: SIP INVITEs with no SDP will be generated and sent to this neighbor.
Off: SIP INVITEs will be generated and a pre-configured SDP will be inserted before the INVITEs are sent to this neighbor..
Default: On

Example: `xConfiguration Zones Zone 1 Neighbor Interworking SIP EmptyInviteAllowed : On`

Zones Zone [1..200] Neighbor Interworking SIP Video DefaultBitrate : <64..2048>

Specifies which video bitrate to use when empty INVITEs are not allowed.
Default: 384

Example: `xConfiguration Zones Zone 1 Neighbor Interworking SIP Video DefaultBitrate : 384`

Zones Zone [1..200] Neighbor Interworking SIP Video DefaultCodec : <None/H261/H263/H263p/H263pp/H264>

Specifies which video codec to use when empty INVITEs are not allowed.
Default: H263

Example: `xConfiguration Zones Zone 1 Neighbor Interworking SIP Video DefaultCodec : H263`

Zones Zone [1..200] Neighbor Interworking SIP Video DefaultResolution : <None/QCIF/CIF/4CIF/SIF/4SIF/VGA/SVGA/XGA>

Specifies which video resolution to use when empty INVITEs are not allowed.
Default: CIF

Example: `xConfiguration Zones Zone 1 Neighbor Interworking SIP Video DefaultResolution : CIF`

Zones Zone [1..200] Neighbor Peer [1..6] Address : <S:0..128>

Specifies the IP Address or Fully Qualified Domain Name (FQDN) of the neighbor. If the neighbor zone is a VCS cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 1 Neighbor Peer 1 Address : 192.44.0.18`

Zones Zone [1..200] Neighbor SIP Encryption Mode : <Auto/Off>

Determines whether or not the VCS will allow encrypted SIP calls on this zone.
Auto: SIP calls will be encrypted if a secure SIP transport (TLS) is used.
Off: SIP calls will never be encrypted.
Default: Auto

Example: `xConfiguration Zones Zone 1 Neighbor SIP Encryption Mode : Auto`

Zones Zone [1..200] Neighbor SIP MediaRouting Mode : <Auto/Signaled/Latching>

Specifies how the VCS handles the media for calls to and from this neighbor, and where it will forward the media destined for this neighbor.
Signaled: The media is always taken for calls to and from this neighbor. It will be forwarded as signaled in the SDP received from this neighbor.
Latching: The media is always taken for calls to and from this neighbor. It will be forwarded to the IP Address and port from which media from this neighbor is received.
Auto: Media is only taken if the call is a traversal call. If this neighbor is behind a NAT the VCS will forward the media to the IP Address and port from which media from this zone is received (latching). Otherwise it will forward the media to the IP Address and port signalled in the SDP (signaled).
Default: Auto.

Example: `xConfiguration Zones Zone [1..200] Neighbor SIP MediaRouting Mode : Auto`

Zones Zone [1..200] Neighbor SIP Port: <1024..65534>

Specifies the port on the neighbor to be used for SIP calls to and from this VCS.
Default: 5060

Example: `xConfiguration Zones Zone 1 Neighbor SIP Port: 5060`

Zones Zone [1..200] Neighbor SIP SearchAutoResponse : <On/Off>

Determines what happens when the VCS receives a SIP search that originated as an H.323 search, destined for this zone.
Off: a SIP OPTION message will be sent to the zone.
On: searches will be responded to automatically, without being forwarded to the zone..
Default: Off.

Example: `xConfiguration Zones Zone 1 Neighbor SIP SearchAutoResponse : Off`

Zones Zone [1..200] Neighbor SIP Transport: <UDP/TCP/TLS>

Determines which transport type will be used for SIP calls to and from this neighbor.
Default: TCP

Example: `xConfiguration Zones Zone 1 Neighbor SIP Transport: TCP`

Zones Zone [1..200] SIP Mode: <On/Off>

Determines whether SIP calls will be allowed to and from this zone.
Default: On

Example: `xConfiguration Zones Zone 1 SIP Mode: On`

Zones Zone [1..200] TraversalClient H323 Port: <1024..65534>

Specifies the port on the traversal server to be used for H.323 firewall traversal calls from this VCS. If your traversal server is a VCS Expressway, this must be the port number that has been configured in the Traversal Server zone for this VCS.
Default: 2777

Example: `xConfiguration Zones Zone 2 TraversalClient H323 Port: 2777`

Zones Zone [1..200] TraversalClient H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal server.
Note: the same protocol must be set on the server for calls to and from this traversal client.
Default: Assent

Example: `xConfiguration Zones Zone 2 TraversalClient H323 Protocol: Assent`

Zones Zone [1..200] TraversalClient Peer [1..6] Address : <S:0..128>

Specifies the IP Address or Fully Qualified Domain Name (FQDN) of the traversal server. If the traversal server is a VCS Expressway cluster, this will be one of the peers in that cluster.

Example: `xConfiguration Zones Zone 2 TraversalClient Peer 1 Address : "10.192.168.1"`

Zones Zone [1..200] TraversalClient RetryInterval: <1..65534>

Specifies the interval (in seconds) with which a failed attempt to establish a connection to the traversal server should be retried.
Default: 120

Example: `xConfiguration Zones Zone 2 TraversalClient RetryInterval: 120`

Zones Zone [1..200] TraversalClient SIP Port: <1024..65534>

Specifies the port on the traversal server to be used for SIP calls from this VCS. If your traversal server is a VCS Expressway, this must be the port number that has been configured in the Traversal Server zone for this VCS.
Default: 5060

Example: `xConfiguration Zones Zone 2 TraversalClient SIP Port: 5060`

Zones Zone [1..200] TraversalClient SIP Transport: <TCP/TLS>

Determines which transport type will be used for SIP calls to and from the traversal server.
Default: TCP

Example: `xConfiguration Zones Zone 2 TraversalClient SIP Transport: TCP`

Zones Zone [1..200] TraversalServer Authentication UserName: <S: 1, 128>

The name used by the traversal client when authenticating with the traversal server. If the traversal client is a VCS, this must be the VCS's Authentication User Name. If the traversal client is a gatekeeper, this must be the gatekeeper's System Name. For other types of traversal clients, refer to the VCS Admin Guide for further information.

Example: `xConfiguration Zones Zone 3 TraversalServer Authentication UserName: "User123"`

Zones Zone [1..200] TraversalServer H323 H46019 Demultiplexing Mode: <On/Off>

Determines whether the VCS will operate in Demultiplexing mode for calls from the traversal client.
On: allows use of the same two ports for all calls.
Off: Each call will use a separate pair of ports for media.
Default: Off

Example: `xConfiguration Zones Zone 3 TraversalServer H323 H46019 Demultiplexing Mode: Off`

Zones Zone [1..200] TraversalServer H323 Port: <1024..65534>

Specifies the port on the VCS being used for H.323 firewall traversal from this traversal client.
Default: 6001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 3 TraversalServer H323 Port: 2777`

Zones Zone [1..200] TraversalServer H323 Protocol: <Assent/H46018>

Determines which of the two firewall traversal protocols will be used for calls to and from the traversal client.
Note: the same protocol must be set on the client for calls to and from this traversal server.
Default: Assent

Example: `xConfiguration Zones Zone 3 TraversalServer H323 Protocol: Assent`

Zones Zone [1..200] TraversalServer SIP Port: <1024..65534>

Specifies the port on the VCS being used for SIP firewall traversal from this traversal client.
Default: 7001, incrementing by 1 for each new zone.

Example: `xConfiguration Zones Zone 3 TraversalServer SIP Port: 5060`

Zones Zone [1..200] TraversalServer SIP Transport: <TCP/TLS>

Determines which of the two transport types will be used for SIP calls between the traversal client and VCS.
Default: TCP

Example: `xConfiguration Zones Zone 3 TraversalServer SIP Transport: TCP`

Zones Zone [1..200] TraversalServer TCPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a TCP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
Default: 20

Example: `xConfiguration Zones Zone 3 TraversalServer TCPProbe KeepAliveInterval: 20`

Zones Zone [1..200] TraversalServer TCPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a TCP probe to the VCS.
Default: 5

Example: `xConfiguration Zones Zone 3 TraversalServer TCPProbe RetryCount: 5`

Zones Zone [1..200] TraversalServer TCPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a TCP probe to the VCS.
Default: 2

Example: `xConfiguration Zones Zone 3 TraversalServer TCPProbe RetryInterval: 2`

Zones Zone [1..200] TraversalServer UDPProbe KeepAliveInterval: <1..65534>

Sets the interval (in seconds) with which the traversal client will send a UDP probe to the VCS once a call is established, in order to keep the firewall's NAT bindings open.
Default: 20

Example: `xConfiguration Zones Zone 3 TraversalServer UDPProbe KeepAliveInterval: 20`

Zones Zone [1..200] TraversalServer UDPProbe RetryCount: <1..65534>

Sets the number of times the traversal client will attempt to send a UDP probe to the VCS.
Default: 5

Example: `xConfiguration Zones Zone 3 TraversalServer UDPProbe RetryCount: 5`

Zones Zone [1..200] TraversalServer UDPProbe RetryInterval: <1..65534>

Sets the frequency (in seconds) with which the traversal client will send a UDP probe to the VCS.
Default: 2

Example: `xConfiguration Zones Zone 3 TraversalServer UDPProbe RetryInterval: 2`

Zones Zone [1..200] Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>

Determines the nature of the specified zone, in relation to the Local VCS.
Neighbor: the new zone will be a neighbor of the Local VCS.
TraversalClient: there is a firewall between the zones, and the Local VCS is a traversal client of the new zone.
TraversalServer: there is a firewall between the zones and the Local VCS is a traversal server for the new zone.
ENUM: the new zone contains endpoints discoverable by ENUM lookup.
DNS: the new zone contains endpoints discoverable by DNS lookup.
Default: Neighbor

Example: `xConfiguration Zones Zone 1 Type: Neighbor`

Overview

The `xCommand` group of commands are used to add and delete items and issue system commands.

The following pages list all the `xCommand` commands currently available on the VCS.

To issue a command, type the command as shown, followed by one or more of the given parameters and values. The valid values for each parameter are indicated in the angle brackets following each parameter; these are explained opposite.

To obtain information about using each of the `xCommand` commands from within the CLI:

- type `xCommand` or `xCommand ?` to return all current `xCommand` commands available on the VCS.
- type `xCommand <command>` or `xCommand <command> ?` to return all parameters for that command, along with the valuespace and a description for each.

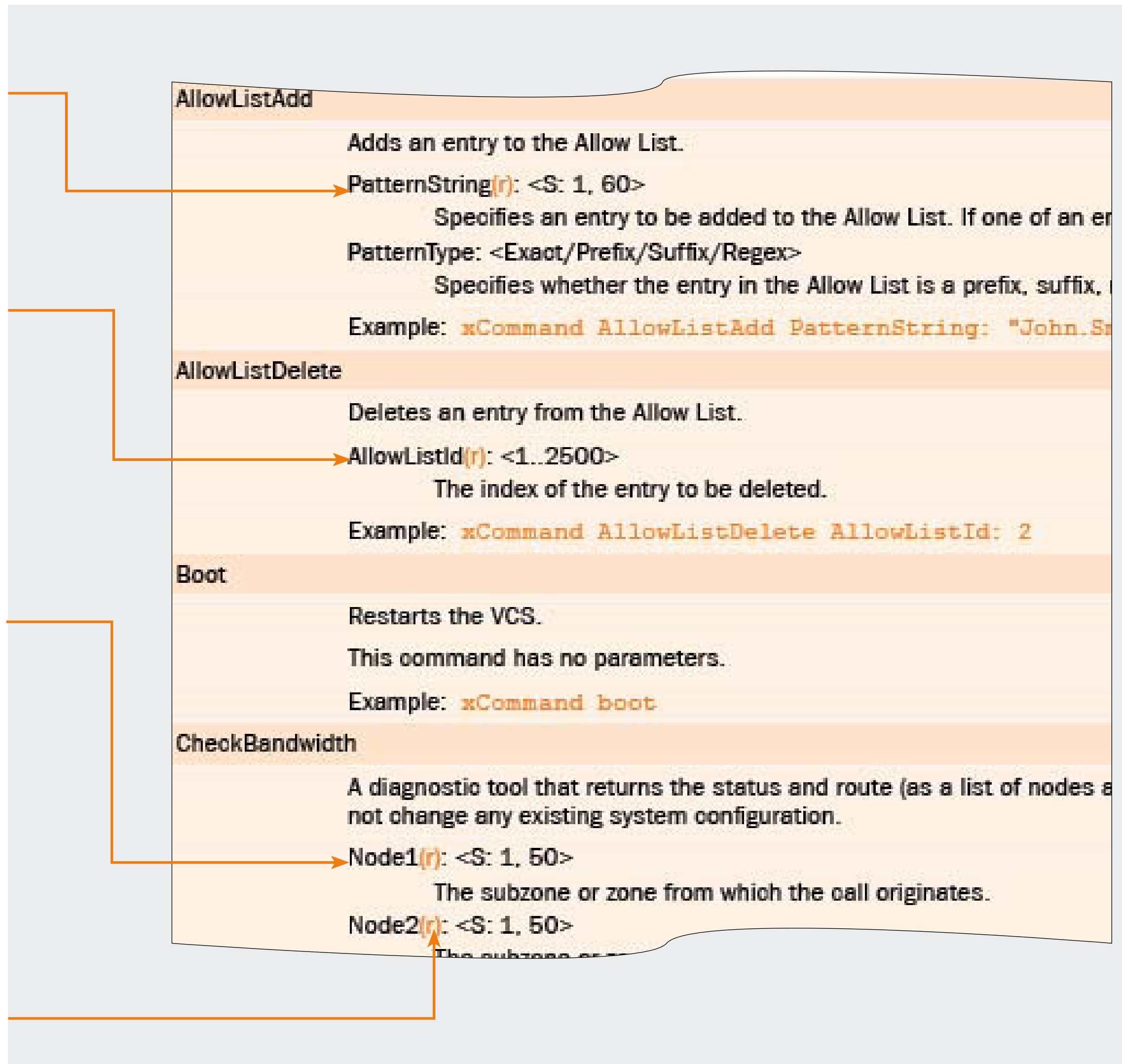
The valid values for this parameter are one of the options shown within the angle brackets.

The valid value for this parameter is an integer. The minimum and maximum values are shown within the angle brackets.

The valid value for this parameter is a string. The minimum and maximum number of characters is shown after the `S`.

When issuing this command, the string must be typed in double quotes.

`(r)` indicates that this is a required parameter. The `(r)` is not part of the command.


AllowListAdd
Adds an entry to the Allow List.
PatternString(r): <S: 1, 60>
Specifies an entry to be added to the Allow List. If one of an en
PatternType: <Exact/Prefix/Suffix/Regex>
Specifies whether the entry in the Allow List is a prefix, suffix,
Example: `xCommand AllowListAdd PatternString: "John.Sm`
AllowListDelete
Deletes an entry from the Allow List.
AllowListId(r): <1..2500>
The index of the entry to be deleted.
Example: `xCommand AllowListDelete AllowListId: 2`
Boot
Restarts the VCS.
This command has no parameters.
Example: `xCommand boot`
CheckBandwidth
A diagnostic tool that returns the status and route (as a list of nodes a
not change any existing system configuration.
Node1(r): <S: 1, 50>
The subzone or zone from which the call originates.
Node2(r): <S: 1, 50>

Command Reference - xCommand

AdminAccountAdd

Creates a new administration account.

Name(r): <S:0..25>
Defines the name of an administration user who can login to the VCS Web interface.
Password(r): <S:0..65>
Defines the password of an administration user who can login to the VCS Web interface. The maximum plaintext length is 16 characters, which will then be encrypted.
Access(r): <Account Disabled/Read Only/Read Write>
Defines the Access level of an administration user who can login to the VCS Web interface. The Access determines whether the user can access the VCS, and if so whether they can change the configuration or just view it.

Example: `xCommand AdminAccountAdd Name: guest Password: password123 Access: read only`

AdminAccountDelete

Deletes an administration account.

AdminAccountId(r): <1..15>
The index of the administration account to be deleted.

Example: `xCommand AdminAccountDelete AdminAccountId: 1`

AllowListAdd

Adds an entry to the Allow List.

PatternString(r): <S: 1, 60>
Specifies an entry to be added to the Allow List. If one of an endpoint's aliases matches one of the patterns in the Allow List, the registration will be permitted.
PatternType: <Exact/Prefix/Suffix/Regex>
Specifies whether the entry in the Allow List is a prefix, suffix, regular expression, or must be matched exactly. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression. Default: Exact.

Example: `xCommand AllowListAdd PatternString: "John.Smith@example.com" PatternType: Exact`

AllowListDelete

Deletes an entry from the Allow List.

AllowListId(r): <1..2500>
The index of the entry to be deleted.

Example: `xCommand AllowListDelete AllowListId: 2`

Boot

Restarts the VCS.

This command has no parameters.

Example: `xCommand boot`

CheckBandwidth

A diagnostic tool that returns the status and route (as a list of nodes and links) that a call of the specified type and bandwidth would take between two nodes. Note that this command does not change any existing system configuration.

Node1(r): <S: 1, 50>
    The subzone or zone from which the call originates.
Node2(r): <S: 1, 50>
    The subzone or zone at which the call terminates.
Bandwidth(r): <1..100000000>
    The requested bandwidth of the call (in kbps).
CallType(r): <Traversal/NonTraversal>
    Whether the call type is Traversal or Non Traversal.

Example: `xCommand CheckBandwidth Node1: "DefaultSubzone" Node2: "UK Sales Office" Bandwidth: 512 CallType: nontraversal`

CheckPattern

A diagnostic tool that allows you to check the result of an alias transform (local or zone) before you configure it on the system. Note that this command does not change any existing system configuration.

Target(r): <S: 1, 60>
    The original alias.
Pattern(r): <S: 1, 60>
    The pattern against which the alias is to be compared.
Type(r): <Exact/Prefix/Suffix/Regex>
    The way in which the pattern must match the alias in order for the transform to be applied.
Behavior(r): <Strip/Replace>
    The way in which the alias will be modified.
Replace: <S: 1, 60>
    (Applies only if Behavior is set to Replace.) The string to be substituted for the part of the alias that matched the pattern.

Example: `xCommand CheckPattern Target: "john.smith@example.net" Pattern: "@example.net" Type: "suffix" Behavior: replace Replace: "@example.com"`

CredentialAdd

Adds an entry to the local authentication database.

CredentialName(r): <S: 1, 128>
    Defines the name for this entry in the local authentication database.
CredentialPassword(r): <S: 1, 128>
    Defines the password for this entry in the local authentication database.

Example: `xCommand CredentialAdd CredentialName: "John Smith" CredentialPassword: "password123"`

CredentialDelete

Deletes an entry from the local authentication database.

CredentialId(r): <1..2500>
The index of the credential to be deleted.

Example: `xCommand CredentialDelete CredentialId: 2`

DefaultLinksAdd

Restores links between the Default Subzone, Traversal Subzone and the Default Zone.

This command has no parameters.

Example: `xCommand DefaultLinksAdd`

DefaultValuesSet

Resets system parameters to default values.

Level(r): <1..3>
The level of system parameters to be reset.
Level 1: will reset most parameters.
Level 2: There are currently no level 2 parameters, so setting that level has the same effect as setting level 1.
Level 3 resets all level 1 and 2 parameters as well as additional parameters. See the section Restoring Default Configuration for full details.

Example: `xCommand DefaultValuesSet Level: 1`

DenyListAdd

Adds an entry to the Deny List.

PatternString(r): <S: 1, 60>
Specifies an entry to be added to the Deny List. If one of an endpoint's aliases matches one of the patterns in the Deny List, the registration will not be permitted.

PatternType: <Exact/Prefix/Suffix/Regex>
Specifies whether the entry in the Deny List is a prefix, suffix, regular expression, or must be matched exactly. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression. Default: Exact.

Example: `xCommand DenyListAdd PatternString: "sally.jones@example.com" PatternType: "exact"`

DenyListDelete

Deletes an entry from the Deny List.

DenyListId(r): <1..2500>
The index of the entry to be deleted.

Example: `xCommand DenyListDelete DenyListId: 2`

DisconnectCall	
	Disconnects a call.
	Call: <1..900> The index of the call to be disconnected. CallSerialNumber: <S: 1, 255> The serial number of the call to be disconnected. Note: you must specify either a call index or call serial number when using this command.
	Example: `xCommand DisconnectCall CallSerialNumber: "6d843434-211c-11b2-b35d-0010f30f521c"`
DomainAdd	
	Adds a SIP domain for which this VCS is authoritative.
	DomainName(r): <S: 1, 128> Specifies a domain for which this VCS is authoritative. The VCS will act as a SIP Registrar and Presence Server for this domain, and will accept registration requests for any SIP endpoints attempting to register with an alias that includes this domain.
	Example: `xCommand DomainAdd DomainName: "example.com"`
DomainDelete	
	Deletes a domain.
	DomainId(r): <1..20> The index of the domain to be deleted.
	Example: `xCommand DomainDelete DomainId: 2`
FeedbackDeregister	
	Deactivates a particular feedback request.
	ID: <1..3> The index of the feedback request to be deactivated.
	Example: `xCommand FeedbackDeregister ID: 1`

FeedbackRegister

Activates notifications on the event or status change(s) described by the Expression(s). Notifications are sent in XML format to the specified URL. Up to 15 Expressions may be registered for each of 3 feedback IDs.

ID: <1..3>
  The ID of this particular feedback request.
URL(r): <S: 1, 256>
  The URL to which notifications are to be sent.
Expression.1..15: <S: 1, 256>
  The events or status change to be notified. Valid Expressions are:
  Status/Ethernet
  Status/NTP
  Status/LDAP
  Status/Feedback
  Status/ExternalManager
  Status/Calls
  Status/Registrations
  Status/Zones
  Event/CallAttempt
  Event/CallConnected
  Event/CallDisconnected
  Event/CallFailure
  Event/RegistrationAdded
  Event/RegistrationRemoved
  Event/RegistrationFailure
  Event/RegistrationChanged
  Event/Bandwidth
  Event/Locate
  Event/ResourceUsage
  Event/AuthenticationFailure.

Example: `xCommand FeedbackRegister ID: 1 URL: " http://192.168.0.1/submitfeedback/" Expression.1: "Status/Calls" Expression.2: "Event/CallAttempt"`

FindRegistration

Returns information about the registration associated with the specified alias. The alias must be registered on the VCS on which the command is issued.

Alias(r): <S: 1, 60>
  The alias that you wish to find out about.

Example: `xCommand FindRegistration Alias: "john.smith@example.com"`

LinkAdd

Adds and configures a new link.

LinkName(r): <S: 1, 50>
 Assigns a name to this link.
Node1: <S: 1, 50>
 Specifies the first zone or subzone to which this link will be applied.
Node2: <S: 1, 50>
 Specifies the second zone or subzone to which this link will be applied.
Pipe1: <S: 1, 50>
 Specifies the first pipe to be associated with this link.
Pipe2: <S: 1, 50>
 Specifies the second pipe to be associated with this link.

Example: `xCommand LinkAdd LinkName: "Subzone1 to UK" Node1: "Subzone1" Node2: "UK Sales Office" Pipe1: "512Kb ASDL"`

LinkDelete

Deletes a link.

LinkId(r): <1..600>
 The index of the link to be deleted.

Example: `xCommand LinkDelete LinkId: 2`

ListPresentities

Returns a list of all the Presentities being watched by a particular Subscriber.

Subscriber(r): <S:1..255>
 The URI of the Subscriber who is watching.

Example: `xCommand ListPresentities Subscriber: john.smith@example.com`

ListSubscribers

Returns a list of all Subscribers who are watching for the presence information of a particular Presentity.

Presentity(r): <S:1..255>
 The URI of the Presentity being watched.

Example: `xCommand ListSubscribers Presentity: mary.jones@example.com`

Command Reference - xCommand

Locate

Runs the VCS's location algorithm to locate the endpoint identified by the given alias, searching locally, on neighbors, and on systems discovered through the DNS system, within the specified number of 'hops'. Results are reported back through the xFeedback mechanism, which must therefore be activated before issuing this command (e.g. `xFeedback register event/locate`).

Alias(r): <S: 1, 60>
    The alias associated with the endpoint you wish to locate.
HopCount(r): <0..255>
    The hop count to be used in the search.
Protocol(r): <H323/SIP>
    The protocol used to initiate the search.

Example: `xCommand Locate Alias: "john.smith@example.com" HopCount: 15 Protocol: SIP`

OptionKeyAdd

Adds a new option key to the VCS. These are added to the VCS in order to add extra functionality, such as increasing the VCS's capacity. Contact your TANDBERG representative for further information.

Key(r): <S: 0, 90>
    Specifies the option key of your software option.

Example: `xCommand OptionKeyAdd Key: "1X4757T5-1-60BAD5CD"`

OptionKeyDelete

Deletes a software option key from the VCS.

OptionKeyId(r): <1..64>
    Specifies the ID of the software option to be deleted.

Example: `xCommand OptionKeyDelete OptionKeyId: 2`

PipeAdd

Adds and configures a new pipe.

PipeName(r): <S: 1, 50>
    Assigns a name to this pipe.
TotalMode: <Unlimited/Limited/NoBandwidth>
    Determines whether or not this pipe is enforcing total bandwidth restrictions. NoBandwidth: no bandwidth available; no calls can be made using this pipe. Default: Unlimited.
Total: <1..100000000>
    If this pipe has limited bandwidth, sets the maximum bandwidth (in kbps) available at any one time on the pipe. Default: 500000.
PerCallMode: <Unlimited/Limited/NoBandwidth>
    Determines whether or not this pipe is limiting the bandwidth of individual calls. NoBandwidth: no bandwidth available; no calls can be made using this pipe. Default: Unlimited.
PerCall: <1..100000000>
    If this pipe has limited per-call bandwidth, sets the maximum amount of bandwidth (in kbps) available for any one call. Default: 1920.

Example: `xCommand PipeAdd PipeName: "512k ADSL" TotalMode: Limited Total: 512 PerCallMode: Limited PerCall: 128`

PipeDelete

Deletes a pipe.

PipeId(r): <1..100>
The index of the pipe to be deleted.

Example: `xCommand PipeDelete PipeId: 2`

RemoveRegistration

Removes a registration from the VCS.

Registration: <1..3750>
The index of the registration to be removed.
RegistrationSerialNumber: <S: 1, 255>
The serial number of the registration to be removed.

Example: `xCommand RemoveRegistration RegistrationSerialNumber: "a761c4bc-25c9-11b2-a37f-0010f30f521c"`

RouteAdd

Adds and configures a new route.

Address(r): <S: 1, 39>
Specifies an IP Address used in conjunction with the Prefix Length to determine the network to which this route applies.
PrefixLength(r): <1..128>
Specifies the number of bits of the IP Address which must match when determining the network to which this route applies.
Gateway(r): <S: 1, 39>
Specifies the IP Address of the Gateway for this route.
Interface: <Auto/LAN1/LAN2>
Specifies the LAN interface to use for this route. Auto: The VCS will select the most appropriate interface to use. Default: Auto

Example: `xCommand RouteAdd Address: "10.13.8.0" PrefixLength: 32 Gateway: "192.44.0.1"`

RouteDelete

Deletes a route.

RouteId(r): <1..50>
The index of the route to be deleted.

Example: `xCommand RouteDelete RouteId: 1`

SubZoneAdd

Adds and configures a new subzone.

SubZoneName(r): <S: 1, 50>
Assigns a name to this subzone.
Address: <S: 0, 39>
Specifies an IP Address used (in conjunction with the IP Prefix Length) to identify a subnet to be assigned to this subzone.
PrefixLength: <0..128>
Specifies the number of bits of the Subnet IP Address which must match for an IP Address to belong in this subzone.
TotalMode: <Unlimited/Limited/NoBandwidth>
Determines whether the Default Subzone has a limit on the total bandwidth being used by its endpoints at any one time. NoBandwidth: no bandwidth available. No calls can be made to, from, or within the Default Subzone. Default: Unlimited.
Total: <1..100000000>
Sets the total bandwidth limit (in kbps) of the Default Subzone (applies only if Mode is set to Limited). Default: 500000.
PerCallInterMode: <Unlimited/Limited/NoBandwidth>
Determines whether there is a limit on the bandwidth for any one call to or from an endpoint in this subzone. NoBandwidth: no bandwidth available. No calls can be made to or from this subzone. Default: Unlimited.
PerCallInter: <1..100000000>
Specifies the bandwidth limit (in kbps) on any one call to or from an endpoint in this subzone (applies only if Mode is set to Limited). Default: 1920.
PerCallIntraMode: <Unlimited/Limited/NoBandwidth>
Determines whether there is a limit on the bandwidth for any one call between two endpoints within this subzone. NoBandwidth: no bandwidth available. No calls can be made within this subzone. Default: Unlimited.
PerCallIntra: <1..100000000>
Specifies the bandwidth limit (in kbps) for any one call between two endpoints within this subzone (applies only if Mode is set to Limited). Default: 1920.

Example: `xCommand SubZoneAdd SubZoneName: "BranchOffice" Address: "10.13.0.0" PrefixLength: 28 TotalMode: Limited Total: 1024 PerCallInterMode: Limited PerCallInter: 512 PerCallIntraMode: Limited PerCallIntra: 512`

SubZoneDelete

Deletes a subzone.

SubZoneId(r): <1..100>
The index of the subzone to be deleted.

Example: `xCommand SubZoneDelete SubZoneId:2`

Command Reference - xCommand

TransformAdd

Adds and configures a new transform.

Pattern(r): <S: 1, 60>
Specifies the pattern against which the alias is compared.

Type: <Exact/Prefix/Suffix/Regex>
Determines the way in which the string must match the alias. Exact: the string must match the alias character for character. Prefix: the string must appear at the beginning of the alias. Suffix: the string must appear at the end of the alias. Regex: the string will be treated as a regular expression.

Behavior: <Strip/Replace>
Determines how the matched part of the alias will be modified. Strip: the matching prefix or suffix will removed from the alias. Replace: the matching part of the alias will be substituted with the text in the Replace string.

Replace: <S: 1, 60>
(Applies only if pattern behavior is set to Replace.) Specifies the string to be used as a substitution for the part of the alias that matched the pattern.

Priority: <1..65534>
Assigns a priority to the specified transform. Transforms are applied in order of priority, and the priority must be unique for each transform.

Example: `xCommand TransformAdd Pattern: "example.net" Type: suffix Behavior: replace Replace: "example.com" Priority: 3`

TransformDelete

Deletes a transform.

TransformId(r): <1..100>
The index of the transform to be deleted.

Example: `xCommand TransformDelete TransformId: 2`

ZoneAdd

Adds and configures a new zone.

ZoneName(r): <S: 1, 50>
Assigns a name to this zone.

Type(r): <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>
Determines the nature of the specified zone, in relation to the Local VCS. Neighbor: the new zone will be a neighbor of the Local VCS. TraversalClient: there is a firewall between the zones, and the Local VCS is a traversal client of the new zone. TraversalServer: there is a firewall between the zones and the Local VCS is a traversal server for the new zone. ENUM: the new zone contains endpoints discoverable by ENUM lookup. DNS: the new zone contains endpoints discoverable by DNS lookup. Default: Neighbor.

Example: `xCommand ZoneAdd ZoneName: "UK Sales Office" Type: Neighbor`

ZoneDelete

Deletes a zone.

ZoneId(r): <1..200>
The index of the zone to be deleted.

Example: `xCommand ZoneDelete ZoneId: 2`

ZoneList

A diagnostic tool that returns the list of zones (grouped by priority) that would be queried, and any transforms that would be applied, in a search for a given alias. Note that this command does not change any existing system configuration.

Alias(r): <S: 1, 60>

The alias to be searched for.

Example: `xCommand ZoneList Alias: "john.smith@example.com"`

Command Reference - xStatus

Overview

The `xStatus` group of commands are used to return information about the current status of the VCS. Each `xStatus` element returns information about one or more sub-elements.

The following pages list all the `xStatus` commands currently available on the VCS, and the information that is returned by each.

To obtain information about the existing status on the VCS:

- type `xStatus` to return the current status of all status elements on the VCS.
- type `xStatus <element>` to return the current status for that particular element and all its sub-elements.
- type `xStatus <element> <sub-element>` to return the current status of that group of sub-elements.

To obtain information about the `xStatus` commands:

- type `xStatus ?` to return a list of all elements available under the `xStatus` command.

Command Reference - xStatus

SystemUnit:

- Product: TANDBERG VCS
- Uptime: <Time in seconds>
- SystemTime: <Time not set/date-time>
- TimeZone: <GMT or one of 300 other timezones>
- LocalTime: <local-date-time>
- Software:
  - Version: X3.0
  - Build: <Number/Uncontrolled>
  - Name: “Release”
  - ReleaseDate: <Date>
  - ReleaseKey <ReleaseKey>
  - Configuration:
    - NonTraversalCalls: <0..500>
    - TraversalCalls: <0..100>
    - Registrations: <0..2500>
    - Expressway: <True/False>
    - Encryption: <True/False>
    - Interworking: <True/False>
    - UserPolicy: <True/False>
    - DeviceProvisioning: <True/False>
    - DualNetworkInterfaces: <True/False>
  - Hardware:
    - Version: 1.0
    - SerialNumber: <hardware serial number>

Command Reference - xStatus

Ethernet [1..2]:

- MacAddress: <S: 17>
- Speed: <10half/10full/100half/100full/1000full/down>
- IPv4:
  - Address: <IPv4Addr>
  - SubnetMask: <IPv4Addr>
- IPv6:
  - Address: <IPv6Addr>

Options:

- Option [1-64]:
  - Key: <S: 1, 90>
  - Description: <S: 1, 128>

IP:

- Protocol: <IPv4/IPv6/Both>
- IPv4:
  - Gateway: <IPv4Addr>
- IPv6:
  - Gateway: <IPv6Addr>
- DNS:
  - Server [1-5]:
    - Address: <IPv4Addr/IPv6Addr>
  - Domain: <S: 0, 128>

NTP:
Status: <Inactive/Initializing/Active/Failed>
Cause: {Visible if status is Failed} <No response from NTP server/ DNS resolution failed>
Address: <IPv4Addr/IPv6Addr>
Port: <1..65534>
Last Update: <date-time>
Last Correction: <Time in seconds, precision in seconds>

LDAP:
Status: <Inactive/Initializing/Active/Failed>
Cause: {Visible if status is Failed} <Failed to connect to LDAP server / The LDAP server does not support TLS. / Failed to establish a TLS connection to the LDAP server. Please check that the LDAP server certificate is signed by a CA, and that CA is included on the CA certificate installed on the VCS. / Failed to authenticate with LDAP server / A valid CA certificate for the LDAP database has not been uploaded; this is required for connections via TLS / No server address configured>
Address: <IPv4Addr/IPv6Addr>
Port: <1..65534>

External Manager:
Status: <Inactive/Initializing/Active/Failed>
Cause: {Visible if status is Failed} <Failed to connect to external manager / No response from external manager / Failed to register to external manager / DNS resolution failed >
Address: <IPv4Addr/IPv6Addr >
Protocol: HTTP
URL: <S: 0, 255>

Feedback [1..3]:
Status: <On/Off>
URL: <S: 1,255>
Expression: <S: 1,127> {0..15 entries}

- **ResourceUsage:**
  - Calls:
    - Traversal:
      - Current: <0..150>
      - Max: <0..150>
      - Total: <0..4294967295>
    - NonTraversal:
      - Current: <0..750>
      - Max: <0..750>
      - Total: <0..4294967295>
  - Registrations:
    - Current: <0..3750>
    - Max: <0..3750>
    - Total: <0..4294967295>

- **Calls:**
  - Call <1..900>:
    - SerialNumber: <S: 1,255>
    - State: <Connecting/Connected/Disconnecting>
    - StartTime: <Seconds since boot/Date Time>
    - Duration: <Time in seconds, precision in seconds>
    - Legs:
      - Leg [1..300]:
        - Protocol: <H323/SIP>
        - H323: {visible if Protocol = H323}
          - CallSignalAddress: <IPv4Addr/[IPv6Addr]>:<1..65534>
          - Aliases:
            - Alias [1..50]:
              - Type: <E164/H323Id>
              - Value: <S: 1,60>

- SIP: {visible if Protocol = SIP}
  - Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
  - Transport: <UDP/TCP/TLS/undefined>
  - Aliases:
    - Alias [1..50]:
      - Type: <URL>
      - Value: <S: 1,60>
- EncryptionType: <None/DES/AES-128>
- CheckCode: <S: 1,60> {visible if Leg = H323 and call is interworked}
- Targets:
  - Target [1..1]:
    - Type: <E164/H323Id/URL>
    - Value: <S: 1,60>
- BandwidthNode: <S: 1,50 Node name>
  - Registration:
    - ID: <1..2500>
    - SerialNumber: <S: 1,255>

Sessions:

- Session: [1..300:]
  - Status: <Unknown/Searching/Failed/Cancelled/Completed/Active/Connected>
  - MediaRouted: <True/False>
  - Participants:
    - Leg: <1..300> {2 entries}
  - Bandwidth:
    - Requested: <0..100000000> kbps
    - Allocated: <0..100000000> kbps
  - Route:
    - Zone/Link: <S: 1,50 Node name> {0..150 entries}

Registrations:

- Registration [1..3750]:
  - Protocol: <H323/SIP>
  - Node: <S: 1,50 Node name>
  - SerialNumber: <S: 1,255>
  - CreationTime: <Date Time>
  - Duration: <Time in seconds, precision in seconds>
  - SecondsSinceLastRefresh: <1..65534> {Visible if Protocol is SIP}
  - SecondsToExpiry <1..65534> {Visible if Protocol is SIP}
  - VendorInfo: <S: 1,255>
  - H323: {Visible if Protocol is H323}
    - Type: <Endpoint/MCU/Gateway/Gatekeeper/MCUGateway>:
    - CallSignalAddresses:
      - Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
    - RASAddresses:
      - Address: <IPv4Addr/[IPv6Addr]>:<1..65534>
      - Apparent: <IPv4Addr/[IPv6Addr]>:<1..65534>
    - Prefix: <S: 1,20> {0..50 entries}
    - Aliases:
      - Alias [1..50]:
        - Type: <E164/H323Id/URL/Email/GW Prefix/MCU Prefix/Prefix/Suffix/IPAddress>
        - Origin: <Endpoint/LDAP/Combined>
        - Value: <S: 1,60>
    - Traversal: <Assent/H46018> {Visible for Traversal registration}
  - SIP: {Visible if Protocol is SIP}
    - AOR: <S: 1,128>
    - Contact: <S: 1,255>
    - Path:
      - URI [1..10]: <S: 1,255>

- **Zones:**
  - DefaultZone:
    - Name: “DefaultZone”
    - Bandwidth:
      - LocalUsage: <0..100000000>
      - ClusterUsage: <0..100000000>
    - Calls: {Section visible only if there are calls }
      - Call [0..900]: {0..900 entries}
        - CallId: <S: 1,255>
  - LocalZone:
    - DefaultSubZone:
      - Name: “DefaultSubZone”
      - Bandwidth:
        - LocalUsage: <0..100000000>
        - ClusterUsage: <0..100000000>
      - Registrations: {0..3750 entries } {Section visible only if there are registrations}
        - Registration: <1..3750>
          - SerialNumber: <S: 1,255>
      - Calls: {Section visible only if there are calls}
        - Call [0..900]: {0..900 entries}
          - CallId: <S: 1,255>
    - TraversalSubZone:
      - Name: “TraversalSubZone”
      - Bandwidth:
        - LocalUsage: <0..100000000>
        - ClusterUsage: <0..100000000>
      - Calls: {Section visible only if there are calls }
        - Call [0..900]: {0..900 entries}
          - CallId: <S: 1,255>

- SubZone: [0..100]
  - Name: <S: 1,50 Node name>
  - Bandwidth:
    - LocalUsage: <0..100000000>
    - ClusterUsage: <0..100000000>
  - Registrations: {0..3750 entries} {Section visible only if there are registrations }
    - Registration: <1..3750>
      - SerialNumber: <S: 1,255>
  - Calls: {Section visible only if there are calls}
    - Call [0..900]: {0..900 entries}
      - CallId: <S: 1,255>

Searches:

- Current:
- Total:
- Dropped:

Zone [1..200]:

- Name: <S: 1,50 Node name>
  - Bandwidth:
    - LocalUsage: <0..100000000>
    - ClusterUsage: <0..100000000>
- Status: <Active/Failed/Warning>
- Cause: {Visible if status is Failed or Warning} <System unreachable/ Systems unreachable>
- Type: <Neighbor/TraversalClient/TraversalServer/ENUM/DNS>
- Neighbor: {Visible if Type is Neighbor}
  - Peer [1..6]:
    - H323: {Visible if H323 Mode=On for Zone}
      - Status: <Unknown/Active/Failed>
      - Cause: {Visible if Status is Failed} <No response from gatekeeper/DNS resolution failed/Invalid IP address>
      - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
      - Port: <1..65534>
      - LastStatusChange: <Time not set/Date Time>

        - SIP: {Visible if SIP Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from gatekeeper/DNS resolution failed/Invalid IP address>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>
- TraversalClient: {Visible if Type is TraversalClient}
    - Peer [1..6]:
        - H323: {Visible if H323 Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from gatekeeper/DNS resolution failed/Invalid alias/Authentication Failed/Invalid IP address>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>
        - SIP: {Visible if SIP Mode=On for Zone}
            - Status: <Unknown/Active/Failed>
            - Cause: {Visible if Status is Failed} <No response from neighbor/ DNS resolution failed>
            - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
            - Port: <1..65534>
            - LastStatusChange: <Time not set/Date Time>
- TraversalServer: {Visible if Type is TraversalServer}
    - SIP:
        - Port: <Active/Inactive>
    - H323:
        - Port: <Active/Inactive>

- Peer [1..6]:
  - H323: {Visible if H323 Mode=On for Zone}
    - Status: Active
    - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
    - Port: <1..65534>
    - LastStatusChange: <Time not set/Date Time>
  - SIP: {Visible if SIP Mode=On for Zone}
    - Status: Active
    - Address: <IPv4Addr/IPv6Addr> {One Address line per address from DNS lookup}
    - Port: <1..65534>
    - LastStatusChange: <Time not set/Date Time>
- Calls: {0..900 entries}
  - Call [0..900]:
  - CallID: <S: 1,255>

Links:

- Link [1..100]:
  - Name: <S: 1,50 Link name>
  - Bandwidth:
    - LocalUsage: <0..100000000>
    - ClusterUsage: <0..100000000>
  - Calls:
    - Call [0..900]: {0..900 entries}
      - CallSerialNumber: <S: 1,255>

Pipes:

- Pipe [1..100]:
  - Name: <S: 1,50 Pipe name>
  - Bandwidth:
    - LocalUsage: <0..100000000>
    - ClusterUsage: <0..100000000>

- Calls:
  - Call [0..900]: {0..900 entries}
    - CallID: <S: 1,255>

Alternates:

- Peer [1..6]: {Hidden for Peer [n] when Peer [n] is self}
  - Status: <Active/Failed/Unknown>
  - Cause: {Visible if status is Failed} <No response from gatekeeper/DNS resolution failed/Invalid IP address>
  - Address: <IPv4Addr/IPv6Addr>
  - Port: <1..65534>
  - LastStatusChange: <Seconds since boot/Date Time>

UserPolicyManager:

- Mode: <Off/Local/Remote>
- Status: <Active/Inactive/Unknown> {Visible if Remote}
- Address: <1..1024> {Visible if Remote}

H323:

- Registration:
  - Status: <Active/Inactive/Failed>
  - IPv4: {Visible if Status=Active}
    - Address: <IPv4Addr> {1..2 entries}
  - IPv6: {Visible if Status=Active}
    - Address: <IPv6Addr> {1..2 entries}
  - OutOfResources: <True/False>
- CallSignaling:
  - Status: <Active/Inactive/Failed>
  - IPv4: {Visible if Status=Active}
    - Address: <IPv4Addr> {1..2 entries}
  - IPv6: {Visible if Status=Active}
    - Address: <IPv6Addr> {1..2 entries}

- Assent:
  - CallSignaling:
    - Status: <Active/Inactive/Failed>
    - IPv4: {Visible if Status=Active}
      - Address: <IPv4Addr> {1..2 entries}
    - IPv6: {Visible if Status=Active}
      - Address: <IPv6Addr> {1..2 entries}
- H46018:
  - CallSignaling:
    - Status: <Active/Inactive/Failed>
    - IPv4: {Visible if Status=Active}
      - Address: <IPv4Addr> {1..2 entries}
    - IPv6: {Visible if Status=Active}
      - Address: <IPv6Addr> {1..2 entries}

SIP:

- Ethernet [1..2]
  - IPv4:
    - UDP:
      - Status: <Active/Inactive/Failed>
      - Address: <IPv4Addr>
    - TCP:
      - Status: <Active/Inactive/Failed>
      - Address: <IPv4Addr>
    - TLS:
      - Status: <Active/Inactive/Failed>
      - Address: <IPv4Addr>

- IPv6:
  - UDP:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv6Addr>
  - TCP:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv6Addr>
  - TLS:
    - Status: <Active/Inactive/Failed>
    - Address: <IPv6Addr>

STUN:

- Servers:
  - Discovery:
    - Status: <Active/Inactive>
    - Address: <IPv4Addr/IPv6Addr>
  - Relay:
    - Status: <Active/Inactive>
    - Address: <IPv4Addr/IPv6Addr>
    - Allocations:
      - Count: <0..800>
      - Relay [1..800]:
        - Client: <IPv4Addr/IPv6Addr>
        - RelayAddress: <IPv4Addr/IPv6Addr>
        - CreationTime: <Date Time>
        - ExpireTime: <Date Time>

Command Reference - xStatus

- **Warnings**:
  - Warning [1..n]:
    - Value: <S: 1,255>

- Applications:
  - Presence:
    - UserAgent:
      - Status: <Inactive/Initializing/Active/Failed>
      - Presentity:
        - Count: <0..2500>
    - Server:
      - Publications:
        - Presentities:
          - Count: <0..10000>
          - Max: <0..10000>
          - Presentity [1..10000]:
            - URI: <S: 1,255>
            - Document:
              - Count: <1..10>
      - Subscriptions:
        - Subscribers:
          - Count: <0..n>
          - Max: <0..n>
          - Subscriber [1..2500]:
            - URI: <S: 1,255>
            - Subscription:
              - Count: <1..100>
        - Count: <1..2500>
        - Max: <1..2500>
        - Expired: <1..2500>

Presentities:

Count: <0..10000>

Max: <0..10000>

Presentity [1..10000]:

URI: <S: 1,255>

Subscriber:

Count: <1..100>

Bibliography

Reference	Title	Link
1	ITU Specification: H.235 Security and encryption for H-Series (H.323 and other H.245-based) multimedia terminals	http://www.itu.int/rec/T-REC-H.235/en
2	ITU Specification: H.350 Directory services architecture for multimedia conferencing	http://www.itu.int/rec/T-REC-H.350/en
3	RFC 2782: A DNS RR for specifying the location of services (DNS SRV)	http://www.ietf.org/rfc/rfc2782.txt
4	RFC 3164: The BSD syslog Protocol	http://www.ietf.org/rfc/rfc3164.txt
5	RFC 3880: Call Processing Language (CPL): A Language for User Control of Internet Telephony Services	http://www.ietf.org/rfc/rfc3880.txt
6	DNS and BIND Fourth Edition, Albitz and Liu, O'Reilly and Associates, ISBN: 0-596-00158-4	
7	RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record	http://www.ietf.org/rfc/rfc2915.txt
8	RFC 3761: The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)	http://www.ietf.org/rfc/rfc3761.txt
9	Mastering Regular Expressions, Jeffrey E.F. Friedl, O'Reilly and Associates, ISBN: 1-56592-257-3	
10	RFC 3327: Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts	http://www.ietf.org/rfc/rfc3327.txt
11	Session Traversal Utilities for (NAT) (STUN)	http://tools.ietf.org/html/draft-ietf-behave-rfc3489bis-06
12	Obtaining Relay Addresses from Simple Traversal Underneath NAT (STUN)	http://tools.ietf.org/html/draft-ietf-behave-turn-03
13	RFC 4787: Network Address Translation (NAT) Behavioral Requirements for Unicast UDP	http://www.ietf.org/rfc/rfc4787.txt
14	RFC 4028: Session Timers in the Session Initiation Protocol (SIP)	http://www.ietf.org/rfc/rfc4028.txt
15	ITU Specification: H.323: Packet-based multimedia communications systems	http://www.itu.int/rec/T-REC-H.323/en
16	RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers	http://www.ietf.org/rfc/rfc3263.txt
17	RFC 3550: RTP: A Transport Protocol for Real-Time Applications	http://www.ietf.org/rfc/rfc3550.txt
18	RFC 791: Internet Protocol	http://www.ietf.org/rfc/rfc791.txt
19	RFC 2460: Internet Protocol, Version 6 (IPv6) Specification	http://www.ietf.org/rfc/rfc2460.txt
20	RFC 3261: SIP: Session Initiation Protocol	http://www.ietf.org/rfc/rfc3261.txt
21	RFC 3489: STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)	http://www.ietf.org/rfc/rfc3489.txt
22	XML and Writing CPL for TANDBERG Infrastructure products Rev 1.2	http://www.tandberg.com/collateral/documentation/Application_Programmer_Interfaces/XML%20and%20Writing%20CPL%20for%20TANDBERG%20Infrastructure%20Products.pdf
23	Management Information Base for Network Management of TCP/IP-based internets: MIB-II	http://www.ietf.org/rfc/rfc1213.txt

Term	Definition
A record	A type of DNS record that maps a domain name to an IPv4 address.
AAAA record	A type of DNS record that maps a domain name to an IPv6 address.
Administrator Policy	In relation to the VCS, the set of rules configured system-wide (either via the web interface or CPL script) that determine the action(s) to be applied to calls matching a given criteria.
Alias	The name an endpoint uses when registering with the VCS. Other endpoints can then use this name to call it. An endpoint may register with more than one alias.
Alternate	One or more VCSs configured to support the same zone in order to provide redundancy.
AOR Address of Record	A SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the “public address” of the user.
ARQ Admission Request	An endpoint RAS request to make or answer a call.
Assent	TANDBERG’s proprietary protocol for firewall traversal.
Border Controller	A TANDBERG device used to control multimedia networks and firewall traversal.
Call Policy	The set of rules (administrator policy, user policy and transforms) that are applied to a single call to determine whether and how it is placed.
CLI Command Line Interface	A text-based user interface used to access the VCS.
Cluster	A collection of between two and six VCSs that have been configured to work together as a single Local Zone, in order to provide scalability and redundancy.
CPL Call Processing Language	An XML-based language for defining call handling. Defined by RFC 3880 [5].
Default Subzone	A subzone used to represent locally registered endpoints and systems that do not fall within any other existing configured subzones within the Local Zone.
Default Zone	A configurable zone on the VCS used to represent incoming connections from endpoints that are not recognized as belonging to any of the existing configured Neighbor, Traversal Client or Traversal Server Zones.
DNS Domain Name System	A distributed database linking domain names to IP addresses.
DNS zone	On the VCS, a zone used to configure access to endpoints located via a DNS lookup.
E.164	An ITU standard for structured telephone numbers. Each telephone number consists of a country code, area code and subscriber number. For example, TANDBERG’s European Headquarters’ phone number is +47 67 125125, corresponding to a country code of 47 for Norway, area code of 67 for Lysaker and finally 125125 to determine which phone line in Lysaker.
ENUM tElephone NUmber Mapping	A means of mapping E.164 numbers to URIs using DNS.
ENUM zone	On the VCS, a zone used to configure access to endpoints located via ENUM.
External Manager	The remote system that is used to manage endpoints and network infrastructure. The TANDBERG Management Suite (TMS) is an example of an external manager.

Term	Definition
External zone	Any zone configured on the local VCS that connects out to a remote system or the internet. Neighbor, Traversal Server, Traversal Client, ENUM and DNS zones are all external zones.
Firewall traversal	Crossing a firewall or NAT device.
FindMe™	A TANDBERG feature that allows users to have a single alias on which they can be reached regardless of the endpoint(s) they are currently using.
FQDN Fully Qualified Domain Name	A domain name that specifies the node's position in the DNS tree absolutely, uniquely identifying the system or device. Note that in order to use FQDNs instead of IP Addresses when configuring the VCS, you must have at least one DNS server configured.
Gatekeeper	A device used to control H.323 multimedia networks. An example is the TANDBERG Gatekeeper.
Gatekeeper zone	A collection of all the endpoints, gateways and MCUs managed by a single gatekeeper.
H.323	A standard that defines the protocols used for packet-based multimedia communications systems.
HTTP Hypertext Transfer Protocol	A protocol used for communications over the internet.
HTTPS Hypertext Transfer Protocol over Secure Socket Layer	A protocol used for secure communications over the internet, combining HTTP with TLS.
Hop count	The maximum number of gatekeeper or SIP proxy devices (e.g. a VCS) that a message may be forwarded through before it is decided that its intended recipient is not reachable.
ICE Interactive Connectivity Establishment	A collaborative algorithm that works together with STUN services (and other NAT traversal techniques) to allow clients to achieve firewall traversal. This is the emerging traversal standard for use by SIP endpoints (although it could be used for other protocols).
IETF Internet Engineering Task Force	An organization that defines (via documents such as RFCs) the protocol standards and best practices relating to the design, use and management of the internet.
Interworking	Allowing H.323 systems to connect to SIP systems.
IPv4 Internet Protocol version 4	Version 4 of the Internet Protocol, defined in RFC 791 [18].
IPv6 Internet Protocol version 6	Version 6 of the Internet Protocol, defined in RFC 2460 [19].
IRQ Information Request	A request sent to an endpoint requesting information about its status.
LAN Local Area Network	A geographically limited computer network, usually with a high bandwidth throughput.
LDAP Lightweight Directory Access Protocol	A protocol for accessing on-line directories running over TCP/IP.
Link	In relation to the VCS, a connection between two nodes.
Local Registration, Locally Registered Endpoint	A relative term used to refer to any endpoint or system that is registered with the Local VCS.

Term	Definition
Local VCS	A relative term used to refer to the particular VCS that you are currently administering, as opposed to other VCSs in your network.
Local Zone	A relative term used to refer to the group of endpoints and other systems registered to a particular VCS. If a VCS is part of a cluster, the Local Zone refers to the collection of all endpoints and other systems registered to all Peers in that cluster.
LRQ Location Request	A RAS query between gatekeepers to determine the location of an endpoint.
Microsoft OCS 2007	Microsoft OCS (Office Communications Server) 2007 is an enterprise real-time communications server, providing the infrastructure to allow instant messaging, presence, audio-video conferencing and web conferencing functionality.
NAPTR record	A type of DNS record.
NAT Network Address Translation	Also known as IP masquerading. Rewriting source and destination addresses as the IP packet passes through the NAT device.
Neighbor	An remote system to which the VCS has a connection via a Neighbor Zone.
Neighbor zone	On the VCS, a zone used to configure a connection to a remote system with which the Local VCS has a non-traversal relationship.
Node	In relation to the VCS, a node is one end of a link. A node can be a local subzone or a zone.
NTP Network Time Protocol	A protocol used for synchronizing clocks.
Peer	A VCS that has been configured to belong to a Cluster.
PEM Privacy-Enhanced Electronic Mail:	An IETF proposal for securing messages using public key cryptography.
Pipe	In relation to the VCS, a means of controlling the bandwidth used on a link.
Proxy, Proxy Server	In SIP, an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. A proxy server primarily plays the role of routing, which means its job is to ensure that a request is sent to another entity “closer” to the targeted user. Proxies are also useful for enforcing policy (for example, making sure a user is allowed to make a call). A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it. While a proxy can set up calls between SIP endpoints, it does not participate in the call once it is set up.
RAS Registration, Admission and Status	A protocol used between H.323 endpoints and a gatekeeper to register and place calls.
Registrar	In SIP, a server that accepts REGISTER requests and places the information it receives in those requests into the location service for the domain it handles. This information is used to advise other SIP Proxies/Registrars where to send calls for that endpoint.
Regex Regular Expression	A pattern used to match text strings according to a POSIX-defined syntax.
RFC Request for Comments	A process and result used by the IETF for Internet standards.
RS-232	A commonly used standard for computer serial ports.
RTCP RTP Control Protocol	A control protocol for RTP. Defined by RFC 3550 [17].

Glossary

Term	Definition
RTP Real-time Transport Protocol	Real time protocol designed for the transmission of voice and video. Defined by RFC 3550 [17].
SSH Secure Shell	An encrypted protocol used to provide a secure CLI.
SIMPLE Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions	An instant messaging and presence protocol based on SIP.
SIP Session Initiation Protocol	IETF protocol for controlling multimedia communication. Defined by RFC 3261 [20].
SNMP Simple Network Management Protocol	A protocol used to monitor network devices.
Source Alias	The alias present in the “source” field of a message.
SRV record Service record	A type of DNS record.
STUN Simple Traversal of UDP through NATs	Firewall NAT traversal for SIP. Defined by RFC 3489 [21].
Subzone	A segment within a VCS Local Zone.
TCP Transmission Control Protocol	A reliable communication protocol defined by RFC 791 [18].
Telnet	A network protocol used on the internet or Local Area Networks (LANs).
TLS Transport Layer Security	A protocol that provides secure communications over the internet.
TMS TANDBERG Management Suite	A TANDBERG product used for the management of video networks.
Transform	In relation to the VCS, the process of changing or replacing the alias being searched for.
Traversal call	Any call where both signaling and media are routed through the VCS.
Traversal Client	A traversal entity on the private side of a firewall. Examples are a TANDBERG Gatekeeper or TANDBERG VCS Control.
Traversal Client Zone	A zone on a VCS Traversal Client that has been used to configure a connection to a particular Traversal Server.
Traversal Server	A traversal entity on the public side of a firewall. Examples are the TANDBERG Border Controller and the TANDBERG VCS Expressway.
Traversal Server Zone	A zone on a VCS Traversal Server that has been used to configure a connection to a particular Traversal Client.
Traversal Subzone	A conceptual subzone through which all traversal calls are deemed to pass; used to manage the bandwidth of traversal calls.
Traversal-enabled endpoint	Any endpoint that supports the Assent and/or ITU H.460.18 and H.460.19 standards for firewall traversal. This includes all TANDBERG MXP endpoints.

Glossary

Term	Definition
UA User Agent	A SIP device used to make and receive calls.
UDP User Datagram Protocol	A communication protocol defined by RFC 791 [18]. It is less reliable than TCP.
URI Uniform Resource Identifier	A formatted string used to identify a resource, typically on the internet.
User Policy	The set of rules that determine the action(s) to be applied to calls for a particular user or group.
VCS Video Communications Server	A generic term for the TANDBERG product which acts as a gatekeeper and SIP Proxy/Server.
VCS Control	A VCS whose main function is to act as a gatekeeper, SIP proxy and firewall traversal client. This system will generally be located within the firewall.
VCS Expressway	A VCS with the same functionality as a VCS Control that can also act as a firewall traversal server. This will generally be located outside the firewall.
Zone	Zones are used on the VCS to define and configure connections to locally registered and external systems and endpoints. The Local Zone refers to all the locally registered endpoints and systems, and consists of configurable subzones. External zones are used to configure connections to external systems with which the VCS has a Neighbor, Traversal Client or Traversal Server relationship, and to configure the way in which the VCS performs ENUM and DNS searches.

Contact Information

TANDBERG

EUROPEAN HEADQUARTERS

Philip Pedersens vei 20, 1366 Lysaker, Norway

Telephone: +47 67 125 125

Fax: +47 67 125 234

Video: +47 67 126 126

E-mail: tandberg@tandberg.com

U.S. HEADQUARTERS

1212 Avenue of the Americas 24th Floor, New York, NY 10036

Telephone: +1 212 692 6500

Fax: +1 212 692 6501

Video: +1 212 692 6535

E-mail: tandberg@tandberg.com